VES-1624FT-55A

24-port VDSL2 remote IP DSLAM

User's Guide

Version 3.53
9/2008
Edition 1

DEFAULT LOGIN	
IP Address	**http://192.168.0.1 (Out-of-band MGMT port)** **http://192.168.1.1 (In-band ports)**
User Name	**admin**
Password	**1234**

ZyXEL
www.zyxel.com

About This User's Guide

Intended Audience

This manual is intended for people who want to configure the IP DSLAM using the web configurator. You should have at least a basic knowledge of TCP/IP networking concepts and topology.

Related Documentation

It is recommended you use the web configurator to configure the IP DSLAM.

- Supporting Disc
  Refer to the included CD for support documents.
- ZyXEL Web Site
  Please refer to www.zyxel.com for additional support documentation and product certifications.

User Guide Feedback

Help us help you. Send all User Guide-related comments, questions or suggestions for improvement to the following address, or use e-mail instead. Thank you!

The Technical Writing Team,
ZyXEL Communications Corp.,
6 Innovation Road II,
Science-Based Industrial Park,
Hsinchu, 300, Taiwan.

E-mail: techwriters@zyxel.com.tw

Document Conventions

Warnings and Notes

These are how warnings and notes are shown in this User's Guide.

Warnings tell you about things that could harm you or your IP DSLAM.

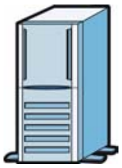
Notes tell you other important information (for example, other things you may need to configure or helpful tips) or recommendations.

Syntax Conventions

- The VES-1624FT-55A may be referred to as the "IP DSLAM", the "device", the "system" or the "product" in this User's Guide.
- Product labels, screen names, field labels and field choices are all in **bold** font.
- A key stroke is denoted by square brackets and uppercase text, for example, [ENTER] means the "enter" or "return" key on your keyboard.
- "Enter" means for you to type one or more characters and then press the [ENTER] key. "Select" or "choose" means for you to use one of the predefined choices.
- A right angle bracket (>) within a screen name denotes a mouse click. For example, **Maintenance** > **Log** > **Log Setting** means you first click **Maintenance** in the navigation panel, then the **Log** sub menu and finally the **Log Setting** tab to get to that screen.
- Units of measurement may denote the "metric" value or the "scientific" value. For example, "k" for kilo may denote "1000" or "1024", "M" for mega may denote "1000000" or "1048576" and so on.
- "e.g.," is a shorthand for "for instance", and "i.e.," means "that is" or "in other words".

Icons Used in Figures

Figures in this User's Guide may use the following generic icons. The IP DSLAM icon is not an exact representation of your IP DSLAM.

IP DSLAM 	Computer 	Notebook computer
Server 	VDSL CPE 	Router
Telephone 	Switch 	Internet / Network

Safety Warnings

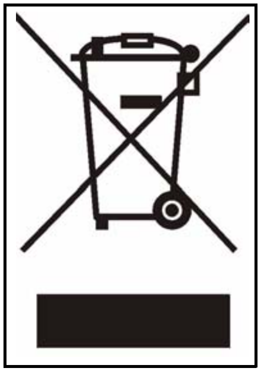
For your safety, be sure to read and follow all warning notices and instructions.

- Do NOT use this product near water, for example, in a wet basement or near a swimming pool.
- Do NOT expose your device to dampness, dust or corrosive liquids.
- Do NOT store things on the device.
- Do NOT install, use, or service this device during a thunderstorm. There is a remote risk of electric shock from lightning.
- Connect ONLY suitable accessories to the device.
- ONLY qualified service personnel should service or disassemble this device.
- Make sure to connect the cables to the correct ports.
- Place connecting cables carefully so that no one will step on them or stumble over them.
- Always disconnect all cables from this device before servicing or disassembling.
- Use ONLY power wires of the appropriate wire gauge (see Chapter 54 on page 283 for details) for your device. Connect it to a power supply of the correct voltage (see Chapter 54 on page 283 for details). .
- Do NOT allow anything to rest on the power adaptor or cord and do NOT place the product where anyone can walk on the power adaptor or cord.
- Do NOT use the device if the power adaptor or cord is damaged as it might cause electrocution.
- If the power adaptor or cord is damaged, remove it from the device and the power source.
- Do NOT attempt to repair the power adaptor or cord. Contact your local vendor to order a new one.
- Do not use the device outside, and make sure all the connections are indoors. There is a remote risk of electric shock from lightning.
- Caution: Risk of explosion if battery (on the motherboard) is replaced by an incorrect type. Dispose of used batteries according to the instructions. Dispose them at the applicable collection point for the recycling of electrical and electronic equipment. For detailed information about recycling of this product, please contact your local city office, your household waste disposal service or the store where you purchased the product.
- Do NOT obstruct the device ventilation slots, as insufficient airflow may harm your device.
- Ensure that the fan filter is in place before switching on the IP DSLAM.
- Use only No. 26 AWG (American Wire Gauge) or larger telecommunication line cord.
- Fuse Warning! Replace a fuse only with a fuse of the same type and rating.
- The length of exposed (bare) power wire should not exceed 7mm.
- Fan Module Warning! Use the fan module handle when pulling out or pushing in the fan module. Be careful not to put fingers or objects inside the fan module.

- The intra-building port(s) of the equipment or subassembly is suitable for connection to intrabuilding or unexposed wiring or cabling only. The intra-building port(s) of the equipment or subassembly MUST NOT be metallically connected to interfaces that connect to the OSP or its wiring. These interfaces are designed for use as intra-building interfaces only (Type 2 or Type 4 ports as described in GR-1089-CORE, Issue 4) and require isolation from the exposed OSP cabling. The addition of Primary Protectors is not sufficient protection in order to connect these interfaces metallically to OSP wiring.

  The intra-building port(s) of the equipment is suitable for connection only to shielded intra-building cabling grounded at both ends.

Your product is marked with this symbol, which is known as the WEEE mark. WEEE stands for Waste Electronics and Electrical Equipment. It means that used electrical and electronic products should not be mixed with general waste. Used electrical and electronic equipment should be treated separately.



Contents Overview

Introduction

Table of Contents

Part V: Troubleshooting and Specifications.................................. 273

Part VI: Appendices and Index 289

List of Figures

List of Tables

PART I
Introduction

1

Introducing the IP DSLAM

This chapter introduces the main applications and features of the IP DSLAM. It also introduces the ways you can manage the IP DSLAM.

1.1 Overview

This chapter describes the system features, applications and specifications of your IP DSLAM.

The IP DSLAM is an IP-based DSLAM (Internet Protocol Digital Subscriber Line Access Multiplexer) that connects VDSL and voice subscribers to the Internet. As a high-performance but yet compact platform, it can conveniently deliver broadband Internet access and VoIP telephony service (over existing POTS telephone wiring) to multi-tenant units (MTUs), hospitals, hotels, schools, university campuses and ISPs. The IP DSLAM's low cost and easy management make it a perfect DSL-provider solution.

The IP DSLAM platform allows for convenient management and support of VDSL technology. Up to 24 VDSL subscribers can simultaneously utilize a wide range of powerful broadband services.

1.2 Applications

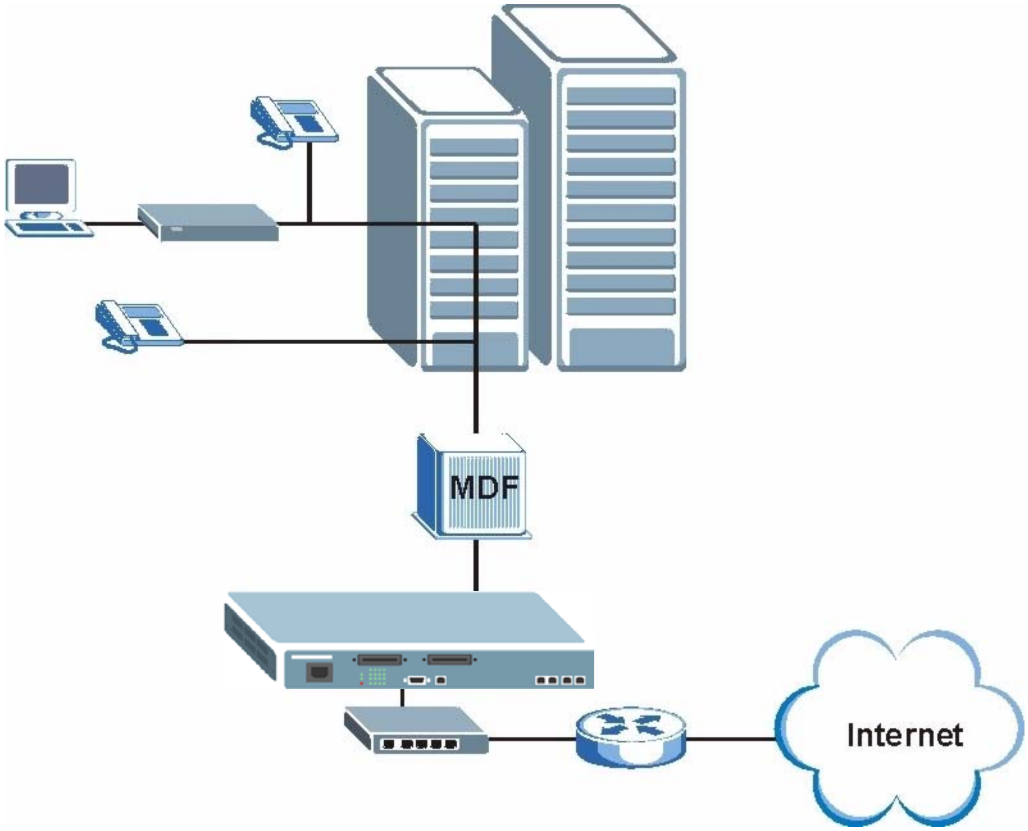
These are the main applications for the IP DSLAM:

- Internet access, multimedia and phone services for Multiple Tenant Units (MTU).
- Other applications include telemedicine, surveillance systems, remote server systems, cellular base stations and high-quality teleconferencing.

1.2.1 MTU Application

The following diagram depicts a typical application of the IP DSLAM with ADSL modems, in a large residential building, or multiple tenant unit (MTU), that leverages existing phone line wiring to provide Internet access and voice service to all tenants. Note that ADSL service can coexist with voice service on the same line.

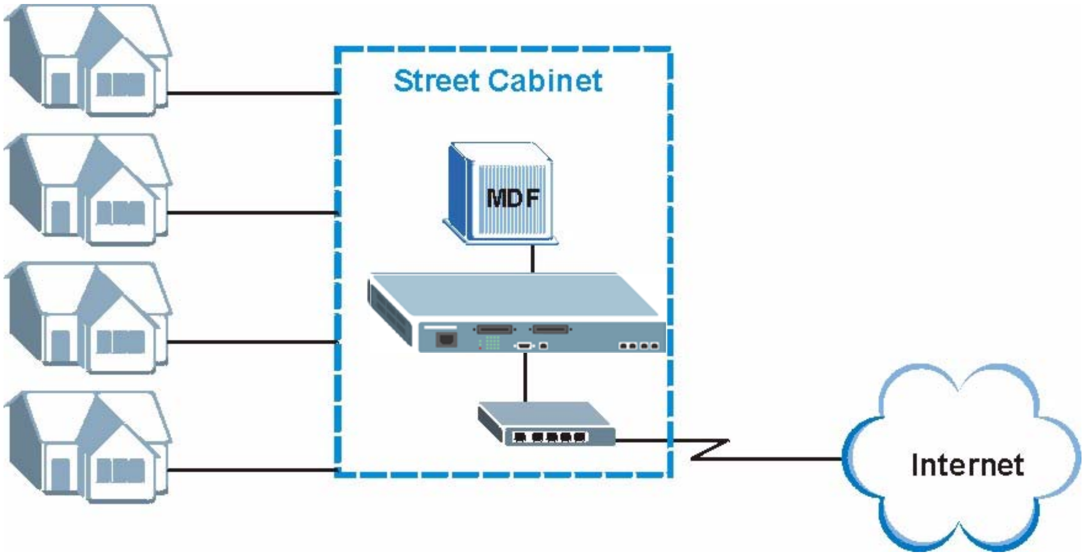
Figure 1 MTU Application



1.2.2 Curbside Application

The IP DSLAM can also be used by an Internet Service Provider (ISP) in a street cabinet to form a “mini POP (Point-of-Presence)” to provide broadband and phone services to residential areas that are too far away from the ISP to avail of DSL or PSTN phone service. Residents need an ADSL modem for data services, connected as shown in the previous figure.

Figure 2 Curbside Application



1.3 Hardware Features

This section describes the ports on the IP DSLAM.

1000/100 Mbps Ethernet Ports

The IP DSLAM has two 1000/100Mbps auto-sensing Ethernet ports.

They allow you to:

- Connect the IP DSLAM to a second-level IP DSLAM
- Daisy-chain other IP DSLAM

SFP Slots

Install SFP (Small Form-factor Pluggable) transceivers in these slots to connect to other IP DSLAMs at longer distances than the Ethernet port.

Stacking

Daisy-chain up to three IP DSLAM (or other Ethernet devices).

Integrated Splitters

The integrated DSL splitter eliminates the need to use external splitters that separate the voice-band and VDSL signals.

Console Port

Use the console port for local management of the IP DSLAM.

Fans

The fans cool the IP DSLAM sufficiently to allow reliable operation of the IP DSLAM in even poorly ventilated rooms or basements. To conserve energy and reduce noise, the fan speed depends on the temperature.

Alarm LED

An **ALM** (alarm) LED lights when the IP DSLAM is overheated, the fans are not working properly, the voltage readings are outside the tolerance levels or an alarm has been detected on the ALARM input pins.

Outband Management Interface

The IP DSLAM has one 10/100 auto-sensing UTP (unshielded twisted pair) port for outband Ethernet Manament.

1.4 Software Features

This section describes the general software features of the IP DSLAM.

System Monitoring

- System status (link status, rates, statistics counters)
- Temperatures, voltage reports and alarms.

DMT Modulation

The IP DSLAM, with the VDSL modem such as P-870H-51 or P-870HW-51, offers service providers a DMT (Discrete Multi-Tone)-based VDSL solution. DMT modulation allows the IP DSLAM to dynamically adapt to the bit rate based on the line condition.

Band Plan Support

Band plan is controlled by Limit PSD Mask (refer to Section 16.4.2 on page 100). All options of Limit PSD Mask for this IP DSLAM follow the band plan defined in G.993.2.The IP DSLAM supports VDSL band Plan.

VDSL Profiles

Profiles allow you to configure VDSL ports efficiently. You can configure all of the VDSL ports with the same profile, thus removing the need to configure the VDSL ports one-by-one. You can also change an individual VDSL port by assigning it a different profile. The [Product Name (long)]

supports the VDSL2 profiles including 8a, 8b, 8c, 8d, 12a, 12b and 17a.

- The DS1 frequency band of the 17a profile starts at 138 kHz and the edge frequency of the upper band of the 17a profile is 17.664 MHz.
- The VDSL2 profiles are programmable and automatically adapt according to the line condition of each VDSL2 line.

IP Protocols

- IP Host (No routing)
- Telnet for configuration and monitoring
- SNMP for management
    - SNMP MIB II (RFC 1213)
    - SNMP v1 RFC 1157
    - SNMPv2, SNMPv2c or later version
    - Bridge MIBs (RFC 1493, 2674)
    - SMI RFC 1155
    - Private MIBs
    - RFC 3728 VDSL MIB

VDSL2 to ADSL2+ Fall Back

The IP DSLAM provides ADSL2+ fall back feature in addition to the VDSL2 PTM (Packet Transmission Mode) service. With ADSL2+ fall back turned on, the IP DSLAM can detect an ADSL modem connected to a subscriber line. Then the IP DSLAM switches the operation mode of the corresponding port to ADSL2+ and establishes the corresponding connection service. This helps Telco operators to provide differentiating services (ADSL service can coexist with VDSL service on the same subscriber line) using a single DSLAM. At the time of writing, the IP DSLAM supports the following features.

- ADSL2+ fall back
- Bi-directional AAL5 ATM VCs
- PPPoA and IPoA/IPoE
- PVC to VLAN mapping

Refer to ITU-T G.992.1, G.992.3 and G.992.5 for more information.

IEEE 802.1Q Tagged VLAN

Your management IP DSLAM card uses the IEEE 802.1Q Tagged VLAN (Virtual Local Area Network), which allows your device to deliver tagged/untagged frames to and from its ports.

IEEE 802.1p Priority

Your IP DSLAM uses IEEE 802.1p Priority to assign priority levels to individual PVCs.

IGMP Count Limit

You can limit the number of IGMP groups a subscriber on a port can join. You may enable/ disable the IGMP count limit on individual ports.

Static Multicast

Use static multicast to allow incoming frames based on multicast MAC address(es) that you specify. This feature can be used in conjunction with IGMP snooping and IGMP proxy to allow multicast MAC address(es) that are not learned by IGMP snooping or IGMP proxy.

Multicast VLAN

Multicast VLAN is designed for applications (such as Media-on-Demand (MoD)) using multicast traffic across an Ethernet ring-based service provider network. Multicast VLAN allows one single multicast VLAN to be shared among different subscriber VLANs on the network. This improves bandwidth utilization by reducing multicast traffic in the subscriber VLANs and simplifies multicast group management.

VLAN Isolation

Use isolation to block the VDSL2 subscribers in a specific VLAN from sending traffic directly to each other.

MAC (Media Access Control) Filter

Use the MAC filter to accept or deny incoming frames based on MAC (Media Access Control) address(es) that you specify. You may enable/disable the MAC filter on specific ports. You may specify up to ten MAC addresses per port.

Security

- Password protection for system management
- VLAN
- RADIUS client

STP (Spanning Tree Protocol) / RSTP (Rapid STP)

(R)STP detects and breaks network loops and provides backup links between IP DSLAMs, bridges or routers. It allows a IP DSLAM to interact with other (R)STP -compliant IP DSLAMs in your network to ensure that only one path exists between any two stations on the network.

IEEE 802.1x Port-based Authentication

The IP DSLAM supports the IEEE 802.1x standard for centralized user authentication and accounting management through an optional network authentication (RADIUS) server.

MAC (Media Access Control) Count Filter

You can limit the number of MAC addresses that may be dynamically learned on a port. You may enable/disable the MAC count filter on individual ports.

DHCP Relay

DHCP (Dynamic Host Configuration Protocol RFC 2131 and RFC 2132) allows individual computers to obtain TCP/IP configuration at start-up from a server. You can configure the system as a DHCP relay agent to have another DHCP server provide TCP/IP configuration for the clients. In addition, you can set the system to forward client DHCP requests to specific DHCP servers based on the VLAN ID. You can also specify up to two DHCP servers for each VLAN to provide fail-over protection.

DHCP Relay Option 82

The system supports DHCP relay agent82 (RFC 3046) that adds additional information to client DHCP requests that the IP DSLAM relays to a DHCP server. It also supports adding the sub-option 2 (Remote ID) with additional information.

DHCP Snooping

DHCP snooping allows the system to identify packets with DHCP server assigned IP address(es) and block access of devices using unknown IP addresses on a subscriber port. You can also manually add static IP addresses to the DHCP snooping table.

2684 Routed Mode

The IP DSLAM can handle 2684 routed mode traffic.

PPPoA-to-PPPoE (PAE) PVC

This feature allows the system to translate PPPoA packets to PPPoE packets (and vice versa) to allow communication between CPE clients and an access concentrator (such as a BRAS) through the IP DSLAM.

DSCP-to-IEEE 802.1p Priority Mapping

DiffServ is a class of service (CoS) model that marks packets with DiffServ Code Points (DSCP) so that they receive specific per-hop treatment at DiffServ-compliant network devices along the route. You can configure DSCP-to-IEEE 802.1p mappings to allow the IP DSLAM to prioritize all incoming traffic based on the DSCP value according to the mapping table.

Transparent LAN Service (TLS)

Use TLS (also known as VLAN stacking) to add an outer VLAN tag to the inner IEEE 802.1Q tagged frames that enter the network. By tagging the tagged frames (“double-tagged” frames), the service provider can manage up to 4,094 VLAN groups with each group containing up to 4,094 customer VLANs. This allows a service provider to provide different services based on specific VLANs, for many different customers.

Downstream Broadcast

The IP DSLAM can block downstream broadcast packets from being sent to specified VLANs on specified ports.

Upstream Broadcast Rate Limiting

Rate Limiting on the subscriber ports allows service providers to offer tiered service in increments of 32 Kbps. This service differentiation is not only to fulfill the needs of different customers, but also to provide a network infrastructure that combines guaranteed performance and flexibility in service provisioning.

System Error Logging

The IP DSLAM’s system error log will record error logs locally. These logs may be viewed again after a warm restart.

Management

- Remote configuration backup/restore and firmware upgrade
- SNMP manageable
- Text-based management locally via console port and remotely via telnet
- Editable plain text based configuration file

PPPoE Intermediate Agent Information

Similar to DHCP relay option82, you can set the system to insert line information into client PPPoE Active Discovery Initialization (PADI) packets. This allows a PPPoE termination server to identify and authenticate a PPPoE client.

Single End Loop Test (SELT)

This feature checks the distance to an ADSL subscriber’s location.

MAC Force Forwarding

This feature forces subscriber(s) to communicate with uplink device(s) through an IPv4 gateway. The gateway then routes or forwards subscriber traffic so the subscribers do not know the MAC addresses of uplink devices on the network. A network administrator can monitor monitor traffic on the gateway. You can also use this feature to distribute traffic through different routers.

2

Hardware Installation

This chapter explains how to install the IP DSLAM.

2.1 General Installation Instructions

Before you begin, read all the safety warnings in Safety Warnings on page 6, and make sure you follow them.

Perform the installation as follows:

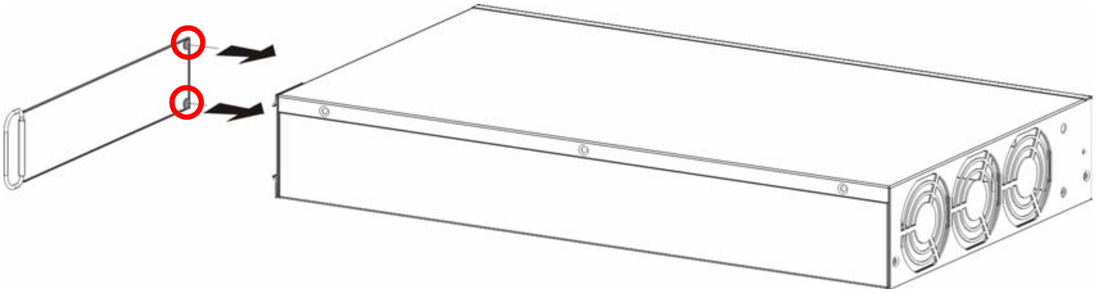
1. Attach the fan dust filter. See Section 2.2 on page 41.
2. Install the hardware. See Section 2.3 on page 42.
3. See Chapter 3 on page 47 for instructions on making front panel connections.
4. See Chapter 4 on page 53 for instructions on connecting the Telco-50 connectors.
5. See Chapter 5 on page 55 for instructions on making power connections and turning on the IP DSLAM.

2.2 Dust Filter Installation

Before you mount the IP DSLAM, take the following steps to install the dust filter.

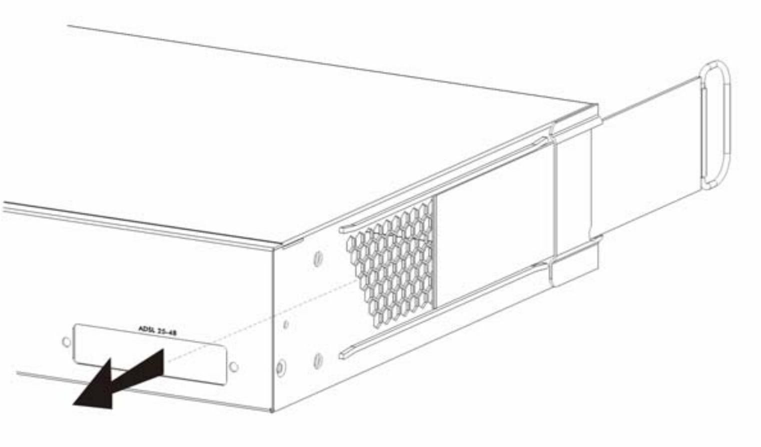
1. Ensure that the side of the dust filter with the magnets is facing the IP DSLAM.

Figure 3 Dust Filter Magnets



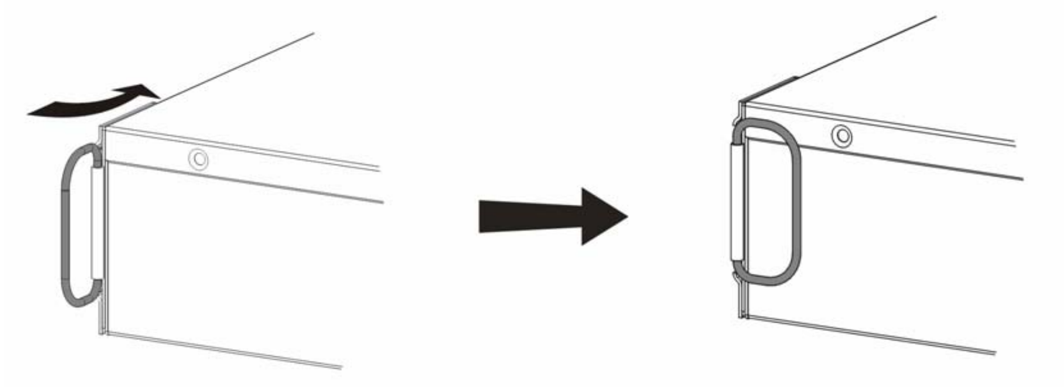
2. Slide the dust filter underneath the dust filter retainer and between the side rails until it is securely fitted on the side of the IP DSLAM.

Figure 4 Dust Filter Installation



3 Flip the dust filter handle around so it is flush with the rear of the IP DSLAM.

Figure 5 Dust Filter Handle



Use the dust filter to prevent dust from getting into the device and possibly damaging it. Clean the dust filter regularly (at least once every two to three months) in order to have sufficient airflow through the device to avoid overheating.

2.3 Installation Scenarios

The IP DSLAM can be placed on a desktop or rack-mounted on a standard EIA rack. Use the rubber feet in a desktop installation and the brackets in a rack-mounted installation.

For proper ventilation, allow at least 4 inches (10 cm) of clearance at the left and right of the IP DSLAM. This is especially important for enclosed rack installations.

2.3.1 Desktop Installation Procedure

1 Make sure the IP DSLAM is clean and dry.

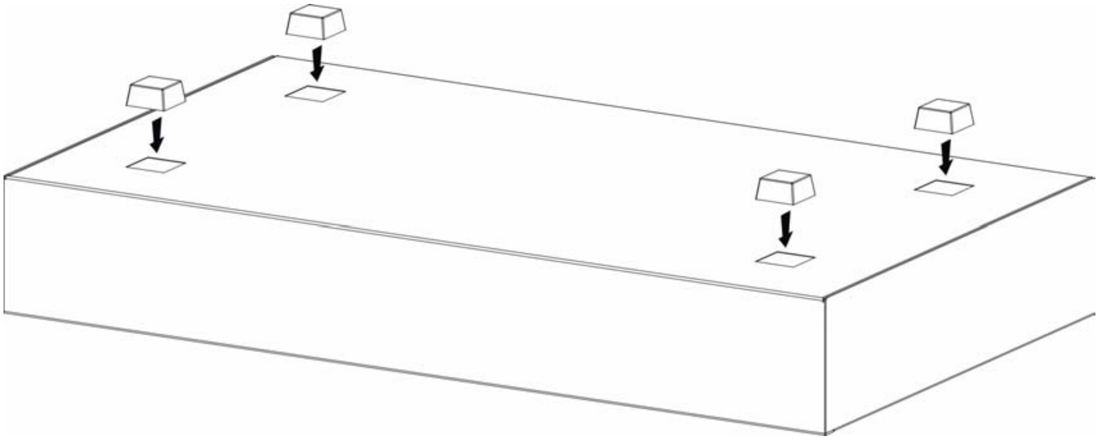
2 Set the IP DSLAM on a smooth, level surface strong enough to support the weight of the IP DSLAM and the connected cables. Make sure there is a power outlet nearby.

3 Make sure there is enough clearance around the IP DSLAM to allow air circulation and the attachment of cables and the power cord.

4 Remove the adhesive backing from the rubber feet.

5 Attach the rubber feet to each corner on the bottom of the IP DSLAM. These rubber feet help protect the IP DSLAM from shock or vibration and ensure space between IP DSLAM when stacking.

Figure 6 Attaching Rubber Feet



Do not block the ventilation holes. Leave space between IP DSLAMs when stacking.

2.3.2 Rack-Mounted Installation

2.3.2.1 Rack-mounted Installation Requirements

The IP DSLAM can be mounted on an EIA standard size, 19-inch rack or in a wiring closet with other equipment. Follow the steps below to mount your IP DSLAM on a standard EIA rack using a rack-mounting kit.

Make sure the rack will safely support the combined weight of all the equipment it contains.

Make sure the position of the IP DSLAM does not make the rack unstable or top-heavy. Take all necessary precautions to anchor the rack securely before installing the unit.

- Use a #2 Phillips screwdriver to install the screws.
- See Chapter 54 on page 283 for the hardware that is required to mount the IP DSLAM.

Failure to use the proper screws may damage the unit.

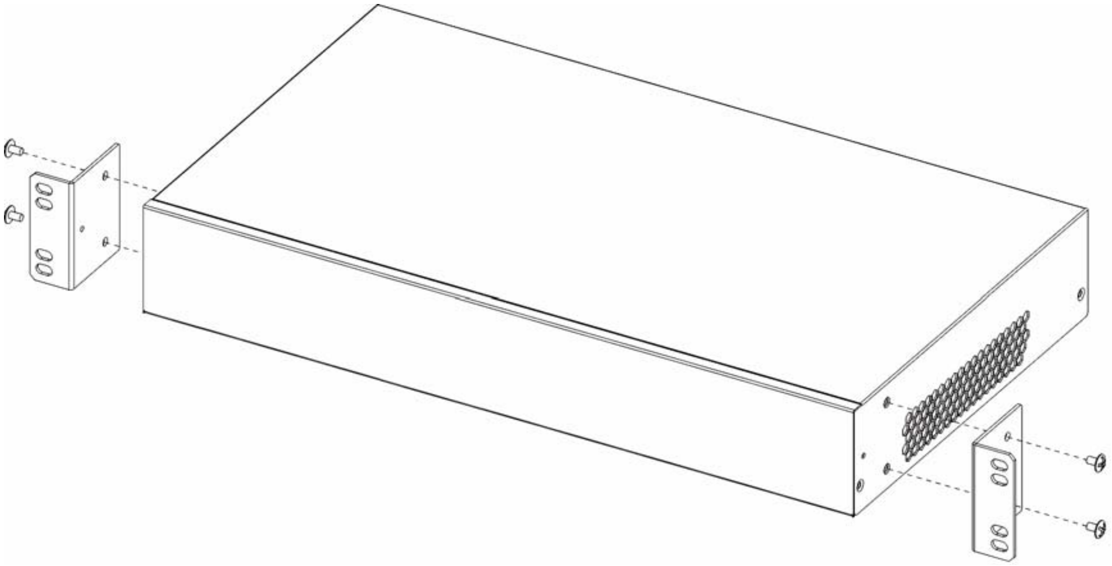
Do not block the ventilation holes. Leave space between IP DSLAM when stacking.

2.3.2.2 Rack-Mounted Installation Procedure

1 Align one bracket with the holes on one side of the IP DSLAM and secure it with the bracket screws smaller than the rack-mounting screws.

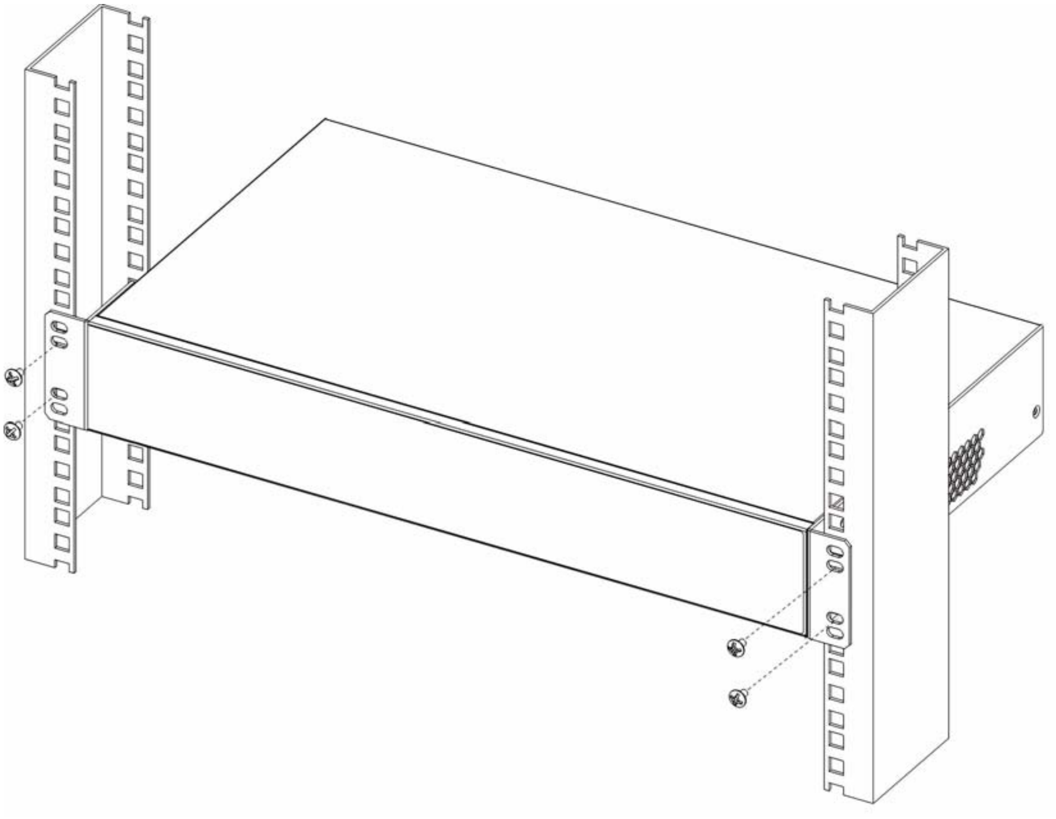
2 Attach the other bracket in a similar fashion.

Figure 7 Attaching Mounting Brackets and Screws



3 After attaching both mounting brackets, position the IP DSLAM in the rack by lining up the holes in the brackets with the appropriate holes on the rack. Secure the IP DSLAM to the rack with the rack-mounting screws.

Figure 8 Rack Mounting



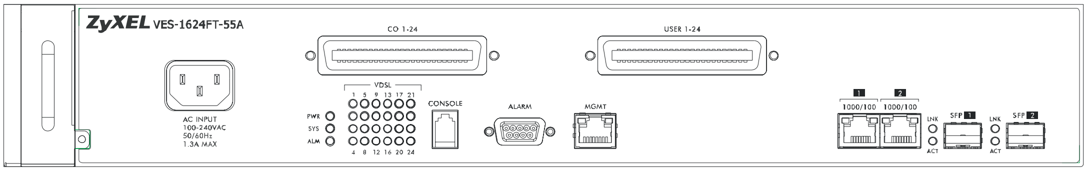
Front Panel Connections

This chapter describes the ports on the front panel, and how to make connections to the ports.

3.1 Front Panel

The following figure shows the front panel of the IP DSLAM.

Figure 9 IP DSLAM Front Panel



3.1.1 Front Panel Ports

The following table describes the ports on the front panel of the IP DSLAM.

Table 1 IP DSLAM Front Panel Ports

CONNECTOR	DESCRIPTION
CO 1-24	Connect a Telco-50 connector to the telephone company for subscribers 1 to 24.
USER 1-24	Connect a Telco-50 connector to DSL subscriber 1 to 24.
CONSOLE	Connect this mini-RJ-11 port to a computer for local management.
ALARM	This DB9 connector has alarm input pins and alarm output pins. Connect the alarm input pins to alarm output terminals on other pieces of equipment. Connect the alarm output pins to an alarm input terminal on another piece of equipment.
MGMT	The RJ-45 port is for local management.
1000/100 1/2	Use these RJ-45 ports for subtending. You can daisy chain more IP DSLAMs or other Ethernet switches. This is an electrical Ethernet interface for use with the following copper Ethernet cables: • 100Base-Tx 2 pair UTP Cat. 5, up to 100m • 1000Base-T 4-pair UTP Cat. 5e or Cat. 6, up to 100m For better performance and lower radiation noise, use shielded Ethernet cables.
SFP 1, 2	Each of these Small Form-factor Pluggable (SFP) slots can house a mini GBIC (Gigabit Interface Converter) transceiver.

3.1.2 Front Panel LEDs

The following table describes the LED indicators on the front panel of the IP DSLAM.

Table 2 LED Descriptions

LED	COLOR	STATUS	DESCRIPTION
PWR	Green	On	The power is turned on.
		Off	The power is off.
SYS	Green	Blinking	The system is rebooting and performing self-diagnostic tests.
		On	The system is on and functioning properly.
		Off	The system is not ready/malfunctioning.
ALM	Red	On	There is a hardware failure or a critical alarm, such as ALM input.
		Off	The system is functioning normally.
1000/100 1,2	Yellow	On	The link to a 100 Mbps Ethernet network is up.
		Blinking	The link is transmitting/receiving 100 Mbps Ethernet traffic.
		Off	The link to a 100 Mbps Ethernet network is down.
	Green	On	The link to a 1000 Mbps (1Gbps) Ethernet network is up.
		Blinking	The link is transmitting/receiving 1000 Mbps (1Gbps) Ethernet traffic.
		Off	The link to a 1000 Mbps (1Gbps) Ethernet network is down.
SFP 1,2 LNK	Green	On	The link to a 1000 Mbps (1 Gbps) Ethernet network is up.
		Off	There is not a link to a 1000 Mbps (1 Gbps) Ethernet network or the 1000 Mbps network link is down.
SFP 1,2 ACT	Green	Blinking	The system is transmitting/receiving Ethernet traffic.
		Off	The system is not transmitting/receiving Ethernet traffic.

3.2 1000/100M Auto-Sensing Ethernet

The IP DSLAM has two 1000/100Mbps auto-sensing Ethernet ports. There are two factors related to Ethernet: speed and duplex mode. In 1000/100Mbps Fast Ethernet, the speed can be 100Mbps or 1000Mbps and the duplex mode can be half duplex or full duplex. The auto-negotiation capability makes one Ethernet port able to negotiate with a peer automatically to obtain the connection speed and duplex mode that both ends support.

When auto-negotiation is turned on, an Ethernet port on the IP DSLAM negotiates with the peer automatically to determine the connection speed and duplex mode. If the peer Ethernet port does not support auto-negotiation or turns off this feature, the IP DSLAM determines the connection speed by detecting the signal on the cable and using half duplex mode. When the IP DSLAM's auto-negotiation is turned off, an Ethernet port uses the pre-configured speed and duplex mode when making a connection, thus requiring you to make sure that the settings of the peer Ethernet port are the same in order to connect.

Use the Ethernet ports for subtending. You can daisy chain more IP DSLAM or other Ethernet switches.

Use with the following copper Ethernet cables: 1000Base-T 4-pair UTP Cat. 5e or Cat.6, up to 100m.

For better performance and lower radiation noise, use shielded Ethernet cables.

Each 1000/100M port is paired with a mini GBIC slot. The IP DSLAM uses up to one connection for each pair for a total of two possible gigabit connections (one from each of the two pairs). The IP DSLAM uses the mini GBIC transceiver whenever it has a connection.

3.2.1 Ethernet Default Settings

- Speed: Auto
- Duplex: Auto

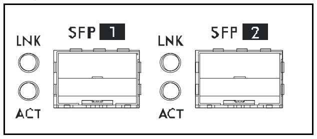
3.3 SFP Mini GBIC Slots

The **SFP** slots can each house a mini GBIC (Gigabit Interface Converter) transceiver. A transceiver is a single unit that houses a transmitter and a receiver. The IP DSLAM does not come with a transceiver. You must use a transceiver that complies with the Small Form-factor Pluggable (SFP) Transceiver MultiSource Agreement (MSA). See the SFF committee’s INF-8074i specification Rev 1.0 for details.

You can change transceivers while the IP DSLAM is operating. You can use different transceivers to connect to Ethernet switches with different types of fiber-optic connectors.

To avoid possible eye injury, do not look directly into an operating fiber-optic module’s connectors.

Figure 10 SFP Mini GBIC Slots



- Type: SFP connection interface
- Connection speed: 1 Gigabit per second (Gbps)

3.3.1 Transceiver Installation

Use the following steps to install a mini GBIC transceiver (SFP module) in the **SFP** slot.

1 Remove the dust cover from the transceiver.

2 For transceivers with a flip-up or flip-down latch, close the latch.

3 Insert the fiber-optic cables into the transceiver (you may need to remove cable dust covers).

4 Insert the transceiver into the IP DSLAM's **SFP** slot.

5 Press the transceiver firmly until it clicks into place.

Figure 11 Transceiver Installation

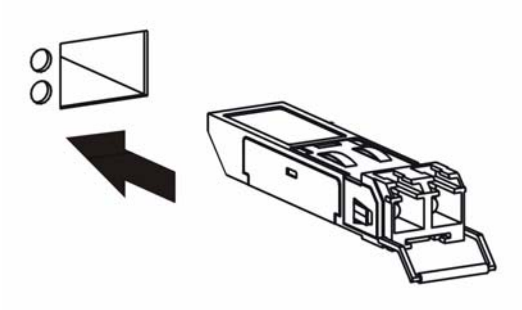
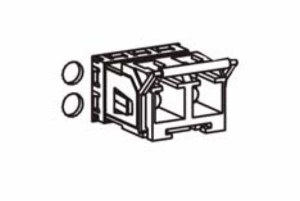


Figure 12 Installed Transceiver



3.3.2 Transceiver Removal

Use the following steps to remove a mini GBIC transceiver (SFP module) from the IP DSLAM.

1 Remove the fiber-optic cables from the transceiver.

2 Unlock the transceiver's latch (latch styles vary).

3 Pull the transceiver out of the slot.

4 Put the transceiver's dust cover on the transceiver.

Figure 13 Opening the Transceiver Latch

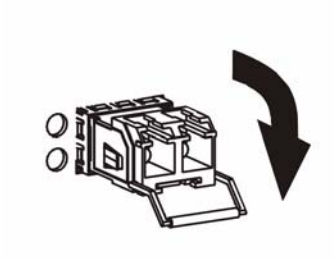
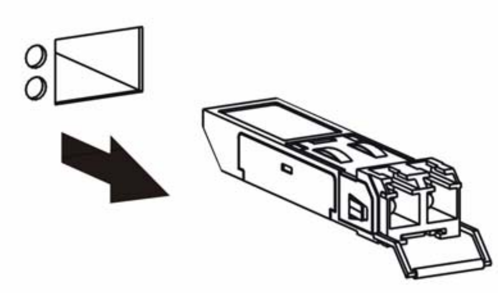


Figure 14 Removing the Transceiver



3.4 Console Port Connection

For local management, you can use a computer with terminal emulation software configured to the following parameters:

- VT100 terminal emulation
- 9600 bps
- No parity, 8 data bits, 1 stop bit
- No flow control

Connect the mini-RJ-11 male end of the console cable to the console port of the IP DSLAM. Connect the female end to a serial port (COM1, COM2 or other COM port) of your computer.

3.5 ALARM Connection

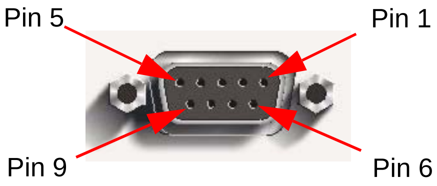
A closed circuit on the **ALARM** input pins indicates an alarm. Pins 7 and 3 are alarm input one. Pins 8 and 4 are alarm input two. Pins 8 and 5 are alarm input 3. Pins 9 and 8 are alarm input 4.

The IP DSLAM signals an alarm when it detects an alarm on the **ALARM** input pins or the IP DSLAM.

To signal an alarm, the IP DSLAM opens the circuit for pins 1 and 6 (the common pin) and closes the circuit for pins 2 and 6.

Examples of an alarm on the IP DSLAM are when the IP DSLAM's voltage or temperature is outside of the normal range.

Figure 15 ALARM Pins Layout



3.6 VDSL Connections

Connect the lines from the user equipment (VDSL/ADSL modems) to the **VDSL** Telco-50 connectors.

The line from the user carries both the VDSL and the voice signals. For each line, the IP DSLAM has a built-in splitter that separates the high frequency VDSL signal from the voice band signal. See Chapter 4 on page 53 for more information on the Telco-50 connections.

4

MDF Connections

This chapter shows you how to connect the Telco-50 connectors to an MDF.

4.1 MDF Connections Overview

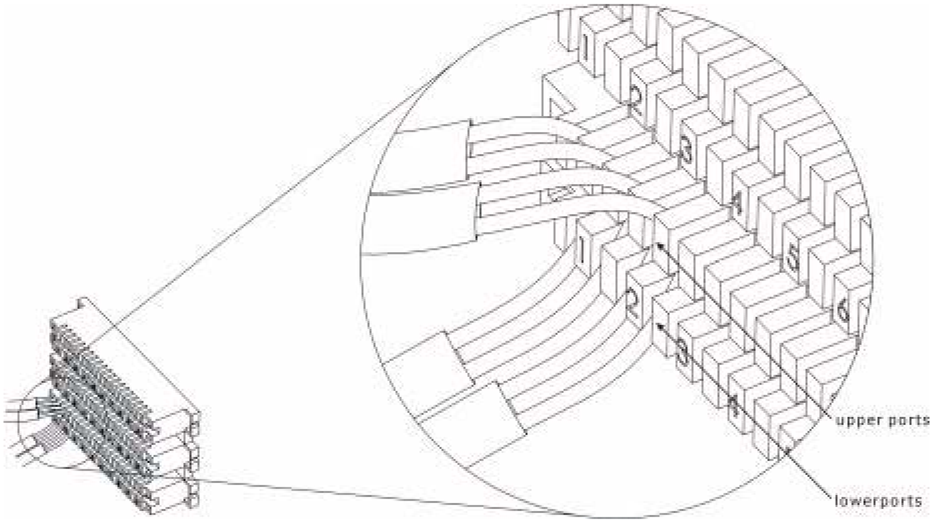
Observe the following before you start:

- See Chapter 54 on page 283 for the gauge of telephone wire to use.
- Follow the pin assignments shown in Chapter 54 on page 283 to wire Telco-50 cables to Telco-50 connectors.
- See Chapter 54 on page 283 for details on how to make the management connections.

4.2 MDF (Main Distribution Frame)

An MDF is usually installed between subscribers' equipment and the telephone company (CO) in a basement or telephone room. The MDF is the point of termination for the outside telephone company lines coming into a building and the telephone wiring in the building.

Figure 16 MDF (Main Distribution Frame) Wiring



- Connect wiring to end-user equipment to the lower ports of an MDF and connect wiring from the telephone company to the upper ports of an MDF (see the previous figure).
- Some MDFs have surge protection circuitry built in between the two banks; thus, do not connect telephone wires from the telephone company directly to your IP DSLAM.

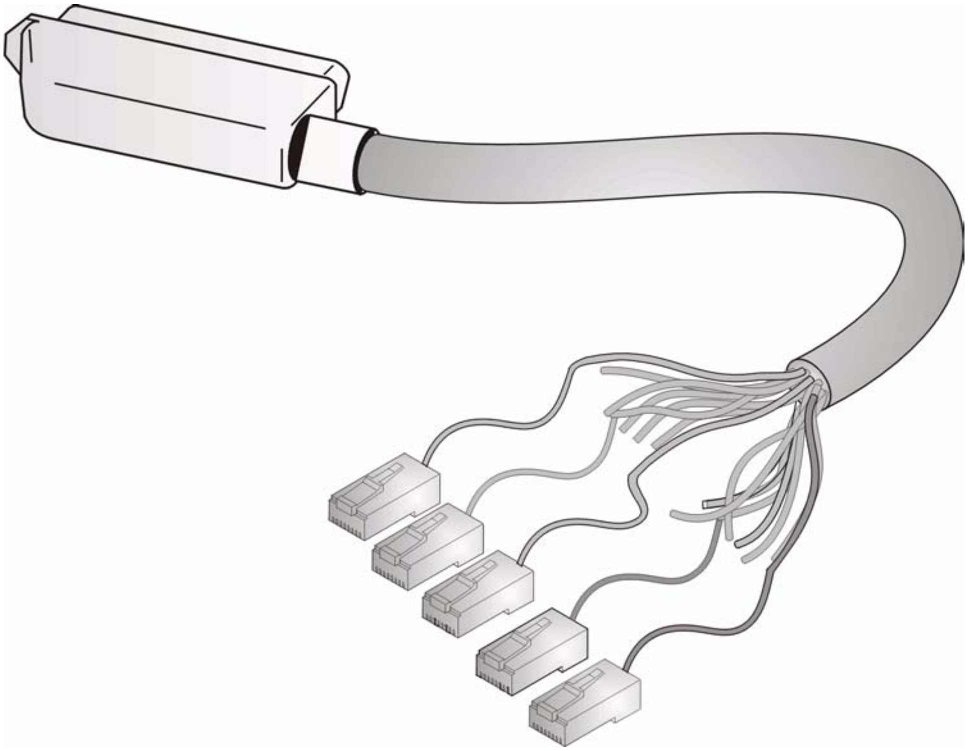
- Use a punch-down tool to seat telephone lines into MDF blocks.
- Multiple upper and lower MDF port connections are shown as one line in the following figures.

4.3 Telco-50 Cables

Telco-50 cables are used for data and voice applications with MDFs (Main Distribution Frame), patch panels and distribution boxes. They can also be used as extension cables. Telco-50 cables are made up of 25 twisted-pair copper wires.

Connect a Telco-50 connector to one end of the cable (see Chapter 54 on page 283 for pin assignments) and connect the other end directly to an MDF; alternatively attach RJ-11 connectors and connect directly to DSL modem(s).

Figure 17 Telco-50 Cable with RJ-11 Connectors



5

Power Connections

This chapter shows you how to connect the IP DSLAM to a power source.

5.1 Power Connections Overview

Use the following procedures to connect the IP DSLAM to a power source after you have installed it in a rack.

Check the power supply requirements in Chapter 54 on page 283, and make sure you are using an appropriate power source.

5.2 Power Connections

The IP DSLAM power connections are at the left side of the front panel.

Use the included power cord to connect the AC power module to the outlet of a compatible power supply. Turn on the power supply to turn on the IP DSLAM.

6

Fan Maintenance

This chapter describes how to change a fan module.

6.1 Fan Maintenance Introduction

The IP DSLAM has a hot-swappable fan module. Use the following procedures to remove the fan module. Replace the entire fan module. Return any malfunctioning fan modules to the manufacturer.

6.2 Removing and Installing the Fan Module

The IP DSLAM fan module is at the left on the front panel. Perform the following procedure to remove the fan module.

1. Loosen the thumbscrew on the front of the fan module.
2. Slide out the fan module.
3. Use a different fan module from the manufacturer.
4. Slide the fan module into the fan module slot.
5. Tighten the thumbscrew.

Figure 18 Fan Module Thumbscrews

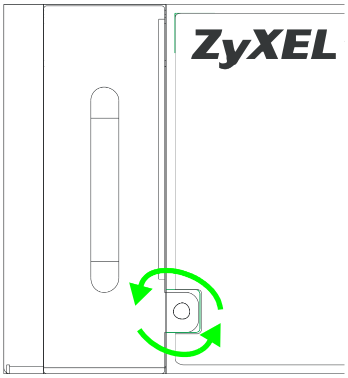


Figure 19 Removing the Fan Module

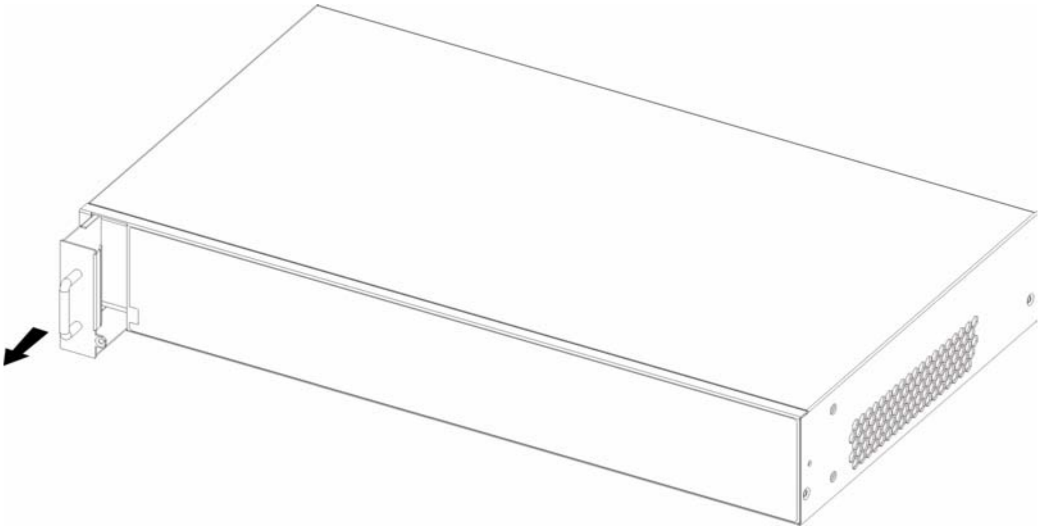
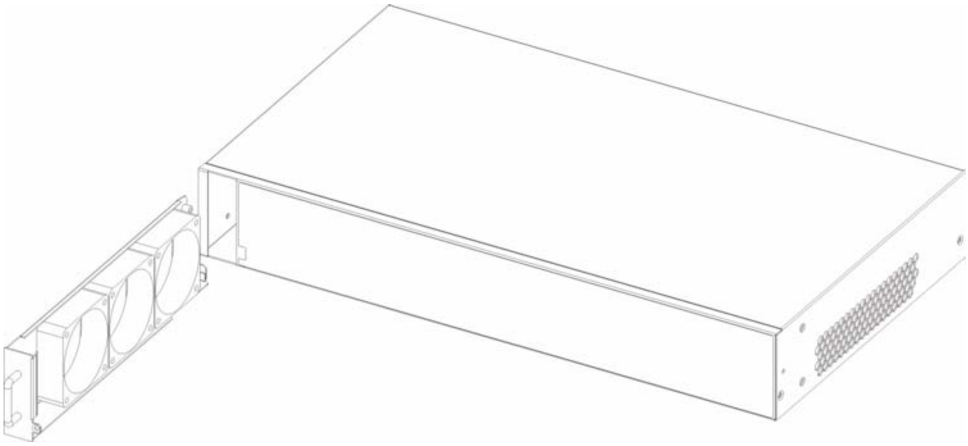


Figure 20 Fan Module Removed



PART II
Basic Settings

7

Introducing the Web Configurator

This chapter tells how to access and navigate the web configurator.

7.1 Web Configurator Overview

The web configurator allows you to use a web browser to manage the IP DSLAM.

7.2 Screen Privilege Levels

There is a high or low privilege level for each screen.

High privilege screens are only available to administrators with high privilege access. High privilege screens include things like creating administrator accounts, restarting the system, saving changes to the nonvolatile memory and resetting to factory defaults. Nonvolatile memory refers to the IP DSLAM's storage that remains even if the IP DSLAM's power is turned off. Administrators with high privilege access can use all screens including the lower privilege screens.

Administrators with the low privilege level are restricted to using only low privilege screens. Low privilege screens are read only.

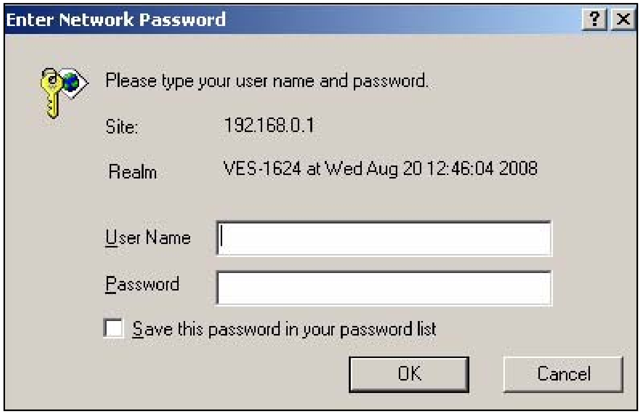
7.3 Accessing the Web Configurator

Use Internet Explorer 6 and later versions with JavaScript enabled.

Use the following instructions to log on to the web configurator.

1 Launch your web browser, and enter the IP address of the IP DSLAM (default: **192.168.0.1** for **MGMT** port or **192.168.1.1** for in-band ports) in the **Location** or **Address** field. Press **Enter**. The **Login** screen appears.

Figure 21 Login



Enter Network Password

Please type your user name and password.

Site: 192.168.0.1

Realm VES-1624 at Wed Aug 20 12:46:04 2008

User Name

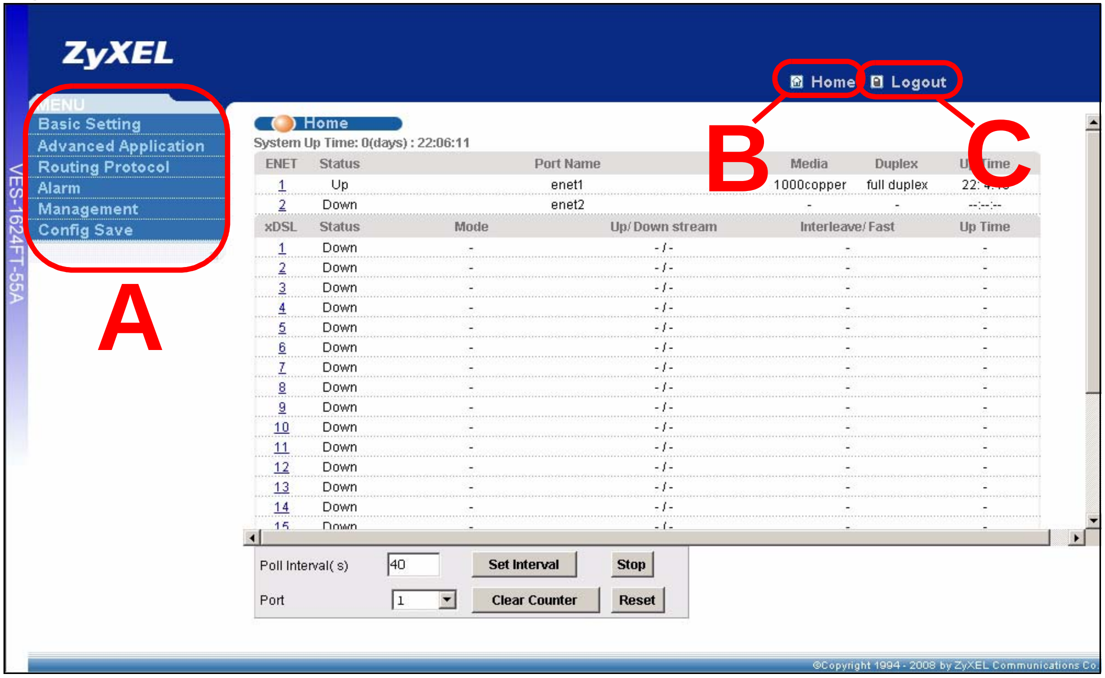
Password

□ Save this password in your password list

2 Type **admin** in the **User Name** field and your password (default: **1234**) in the **Password** field. Click **OK**. The main screen appears.

This is the web configurator's main screen.

Figure 22 Home



System Up Time: 0(days) : 22:06:11

ENET	Status	Port Name	Media	Duplex	Up Time
1	Up	enet1	1000copper	full duplex	22:[illegible]
2	Down	enet2	-	-	--:--:--

xDSL	Status	Mode	Up/ Down stream	Interleave/ Fast	Up Time
1	Down	-	- / -	-	-
2	Down	-	- / -	-	-
3	Down	-	- / -	-	-
4	Down	-	- / -	-	-
5	Down	-	- / -	-	-
6	Down	-	- / -	-	-
7	Down	-	- / -	-	-
8	Down	-	- / -	-	-
9	Down	-	- / -	-	-
10	Down	-	- / -	-	-
11	Down	-	- / -	-	-
12	Down	-	- / -	-	-
13	Down	-	- / -	-	-
14	Down	-	- / -	-	-
15	Down	-	- / -	-	-

Poll Interval(s) 40

Port 1

©Copyright 1994 - 2008 by ZyXEL Communications Co.

A - Click the menu items to open submenu links, and then click on a submenu link to open the screen in the main window. See Section 7.4 on page 63 for more information.

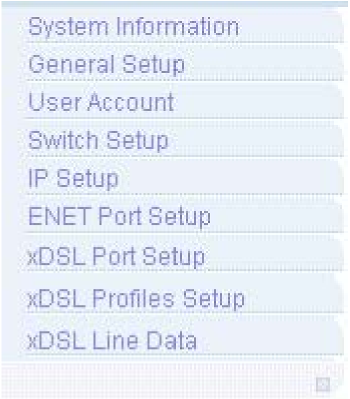
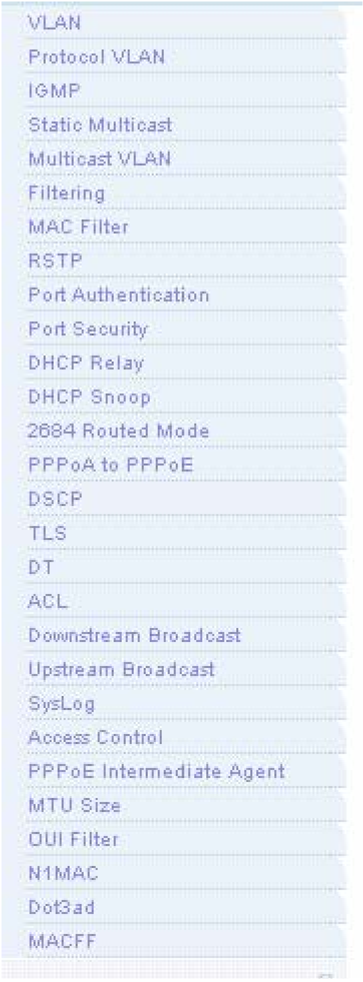
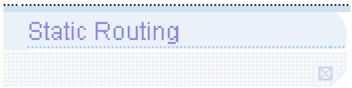
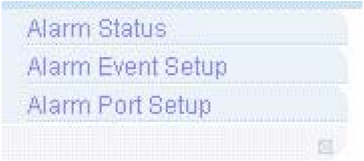
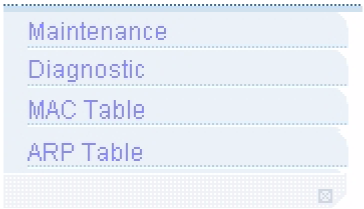
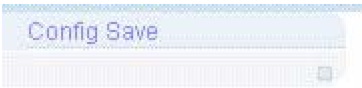
B - Click this to open the **Home** screen. (This is the same screen that is displayed above.) See Chapter 9 on page 73 for more information.

C - Click this to log out of the web configurator.

7.4 Navigation Panel

In the navigation panel, click a menu item to reveal a list of submenu links. Click a submenu link to go to the corresponding screen.

Table 3 Navigation Panel Submenu Links

BASIC SETTING	ADVANCED APPLICATION	ROUTING PROTOCOL
 System Information General Setup User Account Switch Setup IP Setup ENET Port Setup xDSL Port Setup xDSL Profiles Setup xDSL Line Data	 VLAN Protocol VLAN IGMP Static Multicast Multicast VLAN Filtering MAC Filter RSTP Port Authentication Port Security DHCP Relay DHCP Snoop 2684 Routed Mode PPPoA to PPPoE DSCP TLS DT ACL Downstream Broadcast Upstream Broadcast SysLog Access Control PPPoE Intermediate Agent MTU Size OUI Filter N1MAC Dot3ad MACFF	
ALARM	**MANAGEMENT**	**CONFIG SAVE**
		

The following table briefly describes the functions of the screens that you open by clicking the navigation panel’s sub-links.

Table 4 Web Configurator Screens

LABEL	DESCRIPTION
Basic Setting	
System Information	Use this screen to display general system and hardware monitoring information.
General Setup	Use this screen to configure general identification information about the device and the time and date settings.
User Account	Use this screen to configure system administrator accounts.
Switch Setup	Use this screen to set up system-wide parameters such as MAC address learning and priority queues.
IP Setup	Use this screen to configure the system and management IP addresses and subnet masks.
ENET Port Setup	Use this screen to configure settings for the Ethernet ports.
xDSL Port Setup	Use these screens for configuring settings for individual DSL ports.
xDSL Profiles Setup	Use these screens for configuring profiles for the DSL ports.
xDSL Line Data	Use these screens for viewing DSL line operating values, bit allocation and performance counters.
Advanced Application	
VLAN	Use these screens for viewing and configuring the VLAN settings.
Protocol VLAN	Use this screen to configure protocol-based VLAN.
IGMP	Use these screens to view IGMP status information and configure IGMP settings and IGMP filters.
Static Multicast	Use this screen to configure static multicast entries.
Multicast VLAN	Use these screens to set up multicast VLANs that can be shared among different subscriber VLANs on the network.
Filtering	Use this screen to configure packet filtering.
MAC Filter	Use this screen to configure MAC filtering for each port.
RSTP	Use this submenu to go to screens for displaying Rapid Spanning Tree Protocol (RSTP) information and configuring RSTP settings.
Port Authentication	Use this submenu to go to screens for configuring RADIUS and IEEE 802.1x security settings.
Port Security	Use this screen to limit the number of MAC address that can be learned on a port.
DHCP Relay	Use this screen to configure the DHCP relay settings.
DHCP Snoop	Use these screens to drop traffic from IP addresses not assigned by the DHCP server and to look at a summary of the DHCP packets on each port.
2684 Routed Mode	Use this screen to configure the IP DSLAM to handle 2684 routed mode traffic.
PPPoA to PPPoE	Use this screen to enable PPPoA-to-PPPoE conversions on each port.
DSCP	Use this screen to set up DSCP on each port and to convert DSCP values to IEEE 802.1p values.
TLS	Use this screen to set up Transparent LAN Service (VLAN stacking, Q-in-Q) on each port.

Table 4 Web Configurator Screens (continued)

LABEL	DESCRIPTION
DT	Use this screen to configure the VLAN double tagging feature.
ACL	Use this screen to set up Access Control Logic profiles and to assign them to each PVC.
Downstream Broadcast	Use this screen to block downstream broadcast packets from being sent to specified VLANs on specified ports.
Upstream Broadcast	Use this screen to configure the bandwidth for upstream broadcast packets.
SysLog	Use this screen to configure the syslog settings.
Access Control	Use this screen to configure service access control and configure SNMP and remote management.
PPPoE Intermediate Agent	Use this screen to insert line information into client PPPoE Discover Initialization (PADI) packets
MTU Size	Use this screen to configure the Maximum Transmission Unit (MTU) for the Ethernet interfaces. The Ethernet interfaces discard any packets larger than this.
OUI Filter	Use this screen to block or forward packets from devices with the specified OUI (Organizationally Unique Identifier) in the MAC address.
N1MAC	Use this screen to enable multiple-to-one MAC address conversion on specified port(s). Enables this on a port to have the IP DSLAM replace the DSL subscriber device's MAC address with the IP DSLAM's MAC address in upstream traffic flowing through the port. So that the device on the Ethernet network behind the IP DSLAM only see and record the IP DSLAM's MAC address.
Dot3ad	Use this screen to view and configure Ethernet link aggregation settings.
MACFF	Use this screen to configure RFC 4562 MAC force forwarding rules for subscribers. This has matched subscribers then send all traffic through an pre-defined gateway which forwards or routes the subscriber traffic.
Routing	
Static Routing	Use this screen to configure static routes. A static route defines how the IP DSLAM should forward traffic by configuring the TCP/IP parameters manually.
Alarm	
Alarm Status	Use these screens to view the alarms that are currently in the system.
Alarm Event Setup	Use these screens to view and set the severity levels of the alarms and where the system is to send them.
Alarm Port Setup	Use this screen to set the alarm severity threshold for recording alarms on an individual port(s).
Management	
Maintenance	Use this screen to perform firmware and configuration file maintenance as well as restart the system.
Diagnostic	Use this screen to view system logs and test port(s).
MAC Table	Use this screen to view the MAC addresses of devices attached to what ports.
ARP Table	Use this screen to view the MAC address to IP address resolution table.

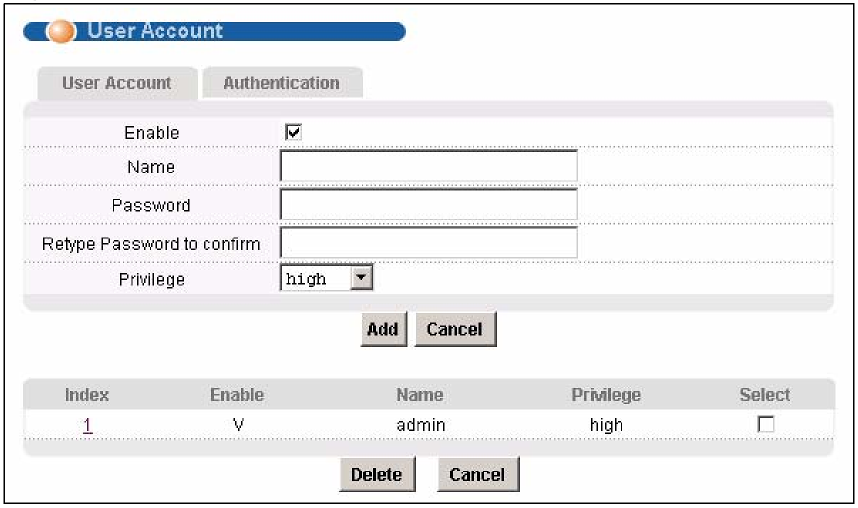
Table 4 Web Configurator Screens (continued)

LABEL	DESCRIPTION
Config Save	
Config Save	Use this screen to save the device's configuration into the nonvolatile memory (the IP DSLAM's storage that remains even if the IP DSLAM's power is turned off).

7.5 Changing Your Password

After you log in for the first time, it is recommended you change the default administrator password. Click **Basic Setting** and then **User Account** to display the **User Account** screen.

Figure 23 User Account

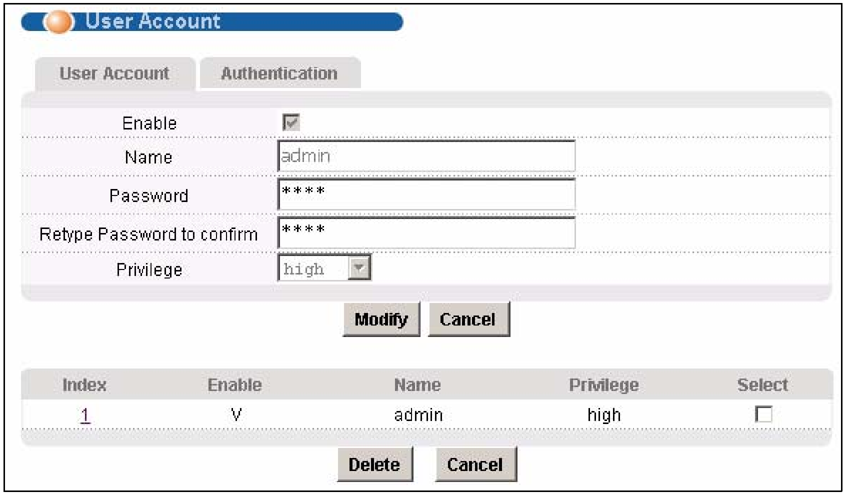


Enable	☑
Name	
Password	
Retype Password to confirm	
Privilege	high

Index	Enable	Name	Privilege	Select
1	V	admin	high	□

Click the index number **1** to edit the default administrator account settings.

Figure 24 User Account



Enable	☑
Name	admin
Password	****
Retype Password to confirm	****
Privilege	high

Index	Enable	Name	Privilege	Select
1	V	admin	high	□

Enter the new password in the **Password** and **Retype Password** to confirm fields, and click **Modify**. Do not forget to click **Config Save** before you exit the web configurator. See Section 7.6 on page 67.

7.6 Saving Your Configuration

Click **Apply** in a configuration screen when you are done modifying the settings in that screen to save your changes back to the run-time memory. Settings in the run-time memory are lost when the IP DSLAM's power is turned off.

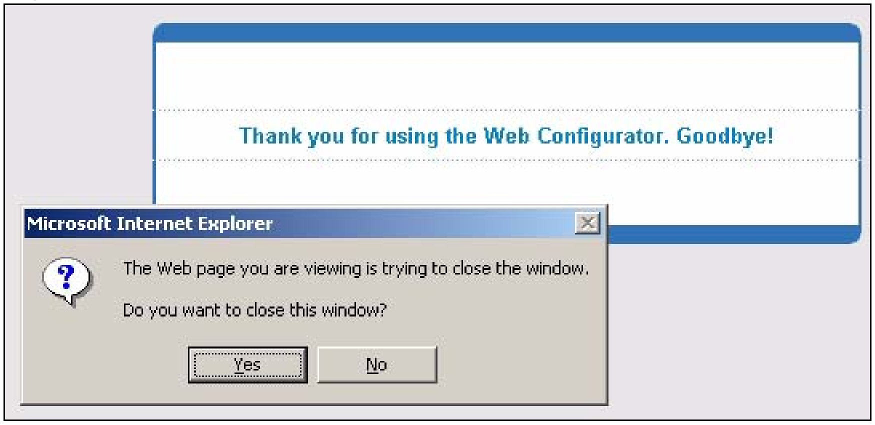
Click **Config Save** in the navigation panel to save your configuration to nonvolatile memory. Nonvolatile memory refers to the IP DSLAM's storage that remains even if the IP DSLAM's power is turned off.

Use **Config Save** when you are done with a configuration session.

7.7 Logging Out of the Web Configurator

Click **Logout** in any screen to exit the web configurator. You have to log in with your password again after you log out. This is recommended after you finish a management session both for security reasons and so you do not lock out other device administrators.

Figure 25 Logout



Thank you for using the Web Configurator. Goodbye!

Microsoft Internet Explorer

The Web page you are viewing is trying to close the window.

Do you want to close this window?

8

Initial Configuration

This chapter describes initial configuration for the IP DSLAM. See Chapter 54 on page 283 for various default settings of the IP DSLAM.

8.1 Initial Configuration Overview

This chapter shows what you first need to do to provide service to VDSL subscribers.

- Switch IP Setup (steps 1~3).
- VDSL Port Setup (steps 4~8).
- Save the Changes (steps 9~10).

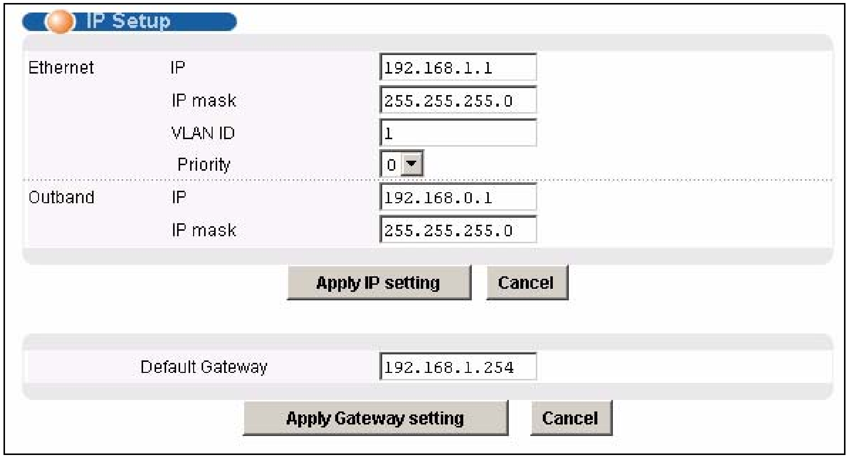
8.2 Initial Configuration

This chapter uses the web configurator for initial configuration. See chapters 53 ~ 68 for information on the commands. Use Internet Explorer 6 and later versions with JavaScript enabled.

1 Log in to the web configurator. See Section 7.3 on page 61 for instructions.

2 In the navigation panel, click **Basic Setting**, **IP Setup**. The **IP Setup** screen appears.

Figure 26 IP Setup



Ethernet	IP	192.168.1.1
	IP mask	255.255.255.0
	VLAN ID	1
	Priority	0
Outband	IP	192.168.0.1
	IP mask	255.255.255.0
	Default Gateway	192.168.1.254

The **Ethernet** IP address (default is 192.168.1.1) is a management IP of the IP DSLAM you can access from the uplink ports. The **Outband** IP address (default is 192.168.0.1) is another management IP you can access through the **MGMT** port.

The **Default Gateway** (default is 192.168.1.254) is used when outgoing traffic needs to be forwarded to another network.

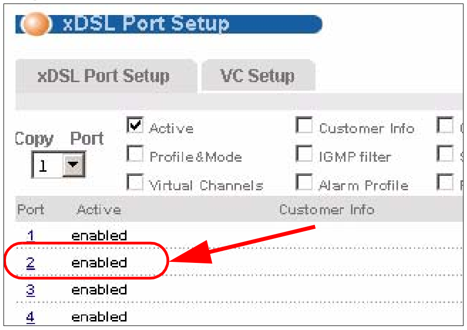
3 Use this screen to change the IP address, subnet mask, and default gateway IP address for your network.

If you change the IP address of the IP DSLAM, after you click **Apply IP setting**, you have to use the new IP address to log into the web configurator again.

4 Activate a VDSL port (for example, port 2) for a VDSL connection.

Click **Basic Setting** > **xDSL Port Setup** and make sure port **2** is enabled (by default, all ports are enabled).

Figure 27 xDSL Port Setup



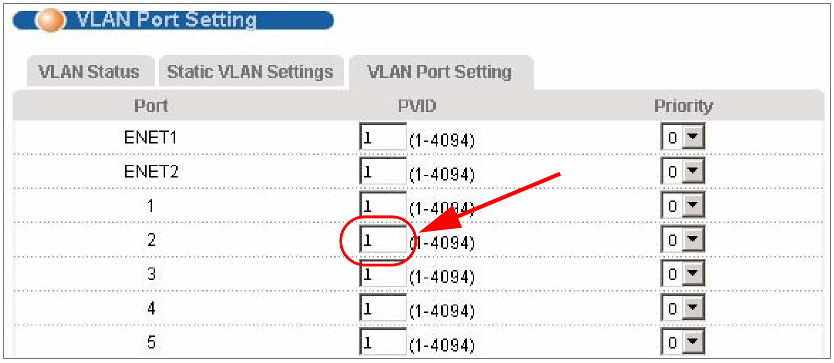
Copy Port 1

☑ Active □ Customer Info □
□ Profile&Mode □ IGMP filter □
□ Virtual Channels □ Alarm Profile □

Port	Active	Customer Info
1	enabled	
2	enabled	
3	enabled	
4	enabled	

5 Click **Advanced Application** > **VLAN** > **VLAN Port Setting**, make sure the PVID of port **2** is PVID **1** (by default, all subscriber ports are members of PVID 1.)

Figure 28 VLAN Port Settings

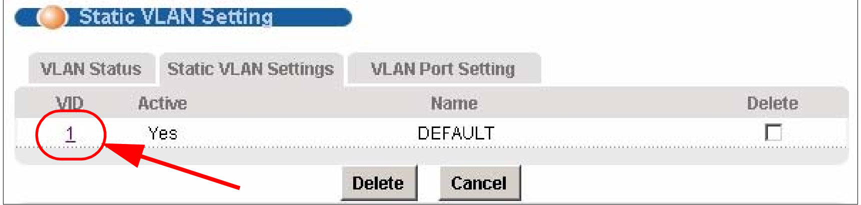


Port	PVID	Priority
ENET1	1 (1-4094)	0
ENET2	1 (1-4094)	0
1	1 (1-4094)	0
2	1 (1-4094)	0
3	1 (1-4094)	0
4	1 (1-4094)	0
5	1 (1-4094)	0

6 Then you have to make sure the port **2** is a member of VLAN **1** (by default, all subscriber ports are members of VLAN 1).

6a Click **Advanced Application > VLAN** > **Static VLAN Settings**, click **VID 1** to bring the settings on the screen.

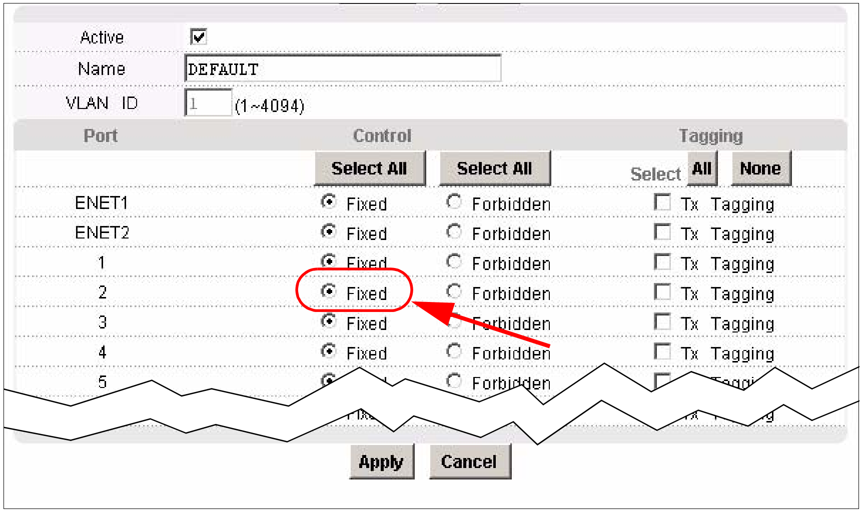
Figure 29 VLAN Port Settings



VID	Active	Name	Delete
1	Yes	DEFAULT	☐

6b Click **Fixed** on port 2 and click **Apply**.

Figure 30 VLAN Port Settings



Active	☑
Name	DEFAULT
VLAN ID	1 (1~4094)

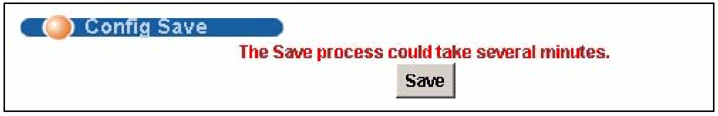
Port	Control		Tagging
ENET1	● Fixed	○ Forbidden	☐ Tx Tagging
ENET2	● Fixed	○ Forbidden	☐ Tx Tagging
1	● Fixed	○ Forbidden	☐ Tx Tagging
2	● Fixed	○ Forbidden	☐ Tx Tagging
3	● Fixed	○ Forbidden	☐ Tx Tagging
4	● Fixed	○ Forbidden	☐ Tx Tagging
5	●	○ Forbidden	☐

7 Connect the subscriber's VDSL device (modem or router) to port **2**. The device should be able to access your network (or the Internet).

8 Repeat steps 4~7 to set up more VDSL subscriber line services.

9 Click **Config Save** > **Config Save**. The **Config Save** screen appears.

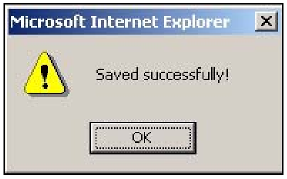
Figure 31 Config Save



The Save process could take several minutes.

10 Click **Save**. The following screen should appear.

Figure 32 Configuration Save Successfully



Saved successfully!

You can now use the device (with the other settings set to the defaults) to provide service to VDSL subscribers. See Chapter 54 on page 283 for information on other default settings.

9

Home and Port Statistics Screens

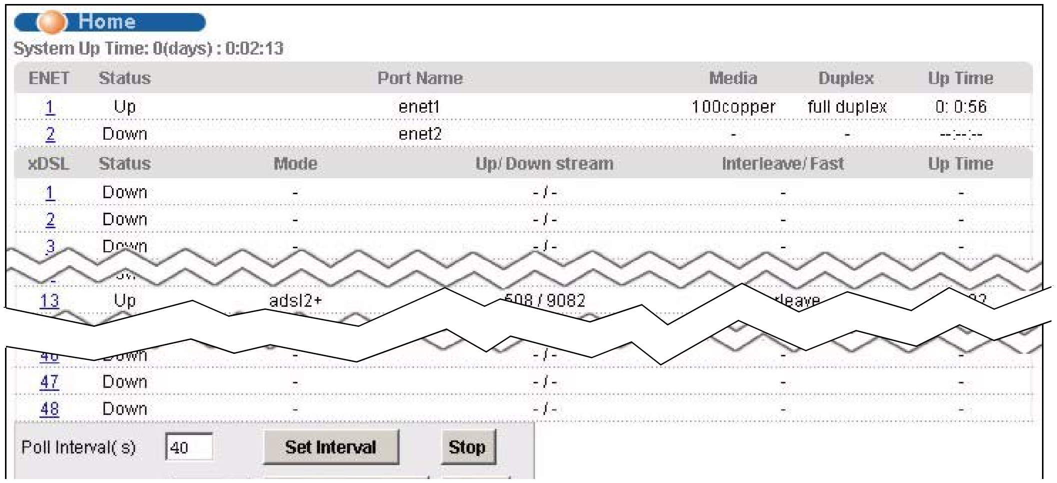
This chapter describes the **Home** (status) and **Port Statistics** screens.

9.1 Home Screen

The **Home** screen of the web configurator displays a port statistical summary with links to each port showing statistical details.

To open this screen, click **Home** in any web configurator screen.

Figure 33 Home



System Up Time: 0(days) : 0:02:13

ENET	Status	Port Name	Media	Duplex	Up Time
1	Up	enet1	100copper	full duplex	0: 0:56
2	Down	enet2	-	-	--:--:--
xDSL	**Status**	**Mode**	**Up/Down stream**	**Interleave/Fast**	**Up Time**
1	Down	-	- / -	-	-
2	Down	-	- / -	-	-
3	Down	-	- / -	-	-
13	Up	adsl2+	508 / 9082	leave	
		-	- / -	-	-
47	Down	-	- / -	-	-
48	Down	-	- / -	-	-

Poll Interval(s) 40

The following table describes the labels in this screen.

Table 5 Home

LABEL	DESCRIPTION
System up Time	This field shows how long the system has been running since the last time it was started.
	The following fields are related to the Ethernet ports.
ENET	This field displays the number of the Ethernet port. Click a port number to display that port's statistics screen. The Ethernet Port Statistics Screen appears. See Section 9.1.1 on page 74.
Status	This field displays whether the Ethernet port is connected (**Up**) or not (**Down**).
Port Name	This field displays the name of the Ethernet port.

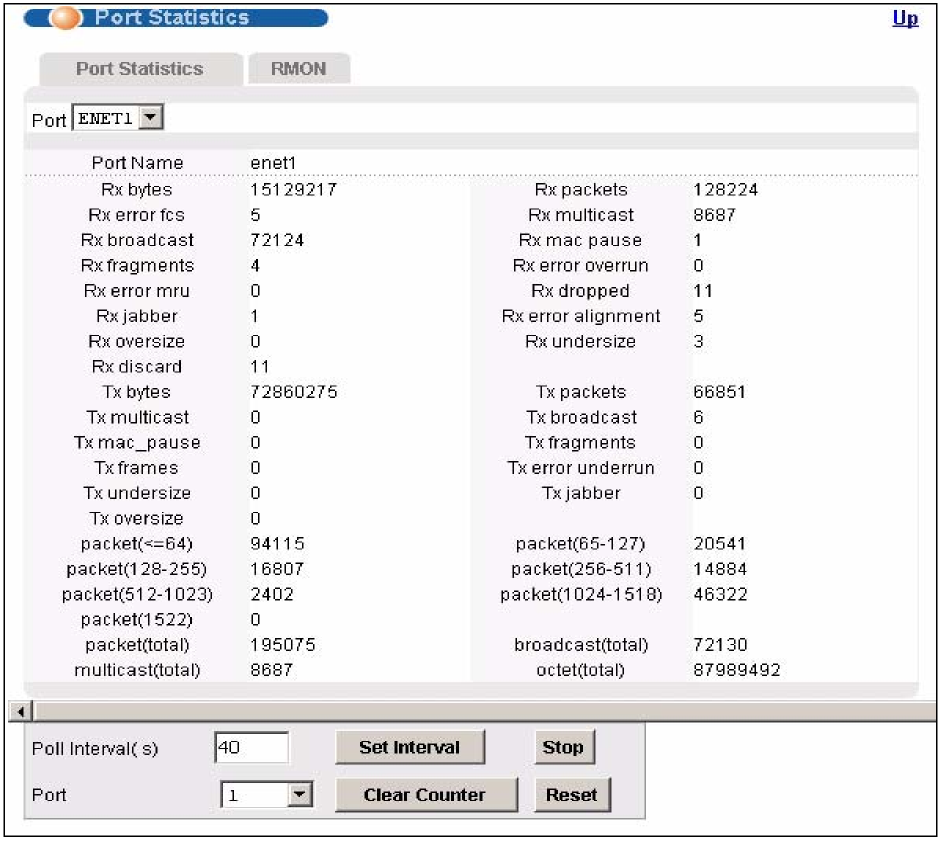
Table 5 Home (continued)

LABEL	DESCRIPTION
Media	This field displays the type of media that this Ethernet port is using for a connection (**copper** or **fiber**). "**-**" displays when the port is disabled or not connected.
Duplex	This field displays whether the port is using **half** or **full duplex** communication. "**-**" displays when the port is disabled or not connected.
Up Time	This field shows the total amount of time in hours, minutes and seconds the port's connection has been up. "**--:--:--**" displays when the port is disabled or not connected.
	The following fields are related to the VDSL ports.
xDSL	This identifies the VDSL port. Click a port number to display that port's statistics screen. The VDSL Port Statistics Screen appears. See Section 9.1.2 on page 77.
Status	This field shows whether the port is connected (**Up**) or not (**Down**).
Mode	This field shows which VDSL operational mode the port is set to use. "**-**" displays when the port is not connected.
Up/Down stream	This field shows the number of kilobits per second that a port is set to transmit and receive. "**-**" displays when the port is not connected.
Interleave/Fast	This field shows the port's VDSL latency mode (**Fast** or **Interleave**). "**-**" displays when the port is not connected.
Up Time	This field shows the total amount of time in hours, minutes and seconds the port's connection has been up. "**-**" displays when the port is not connected.
	The following fields and buttons apply to the whole screen.
Poll Interval(s) Set Interval	The text box displays how often (in seconds) this screen refreshes. You may change the refresh interval by typing a new number in the text box and then clicking **Set Interval**.
Stop	Click **Stop** to halt system statistic polling.
Port Clear Counter	Select a port from the **Port** drop-down list box and then click **Clear Counter** to erase the recorded statistical information for that port.
Reset	Click this to set the **Poll Interval(s)** and **Port** fields to their default values and to refresh the screen.

9.1.1 Ethernet Port Statistics Screen

Use this screen to display statistics about an Ethernet port. To open this screen, click an Ethernet port's number in the **Home** screen.

Figure 34 Port Statistics (Ethernet)



Port ENET1

Port Name	enet1		
Rx bytes	15129217	Rx packets	128224
Rx error fcs	5	Rx multicast	8687
Rx broadcast	72124	Rx mac pause	1
Rx fragments	4	Rx error overrun	0
Rx error mru	0	Rx dropped	11
Rx jabber	1	Rx error alignment	5
Rx oversize	0	Rx undersize	3
Rx discard	11		
Tx bytes	72860275	Tx packets	66851
Tx multicast	0	Tx broadcast	6
Tx mac_pause	0	Tx fragments	0
Tx frames	0	Tx error underrun	0
Tx undersize	0	Tx jabber	0
Tx oversize	0		
packet(<=64)	94115	packet(65-127)	20541
packet(128-255)	16807	packet(256-511)	14884
packet(512-1023)	2402	packet(1024-1518)	46322
packet(1522)	0		
packet(total)	195075	broadcast(total)	72130
multicast(total)	8687	octet(total)	87989492

Poll Interval(s) 40

Port 1

The following table describes the labels in this screen.

Table 6 Port Statistics (Ethernet)

LABEL	DESCRIPTION
Up	Click this to go back to the **Home** screen.
Port	Use this drop-down list box to select a port for which you wish to view statistics. This field identifies the port described in this screen.
Port Name	This field displays the name that you have configured for the port.
Rx bytes	This field shows the number of octets of Ethernet frames received that are from 0 to 1518 octets in size, counting the ones in bad packets, not counting framing bits but counting FCS (Frame Check Sequence) octets. An octet is an 8-bit binary digit (byte).
Rx packets	This field shows the number of packets received on this port (including multicast, unicast, broadcast and bad packets).
Rx error fcs	This field shows the number of frames received with an integral length of 64 to 1518 octets and containing a Frame Check Sequence error.
Rx multicast	This field shows the number of good multicast frames received of 64 to 1518 octets in length (for non VLAN) or 1522 octets (for VLAN), not including Broadcast frames. Frames with range or length errors are also not taken into account.
Rx broadcast	This field shows the number of good broadcast frames received of 64 to 1518 octets in length (for non VLAN) or 1522 octets (for VLAN), not including multicast frames. Frames with range or length errors are also not taken into account.
Rx mac pause	This field shows the number of valid IEEE 802.3x Pause frames received on this port.

Table 6 Port Statistics (Ethernet) (continued)

LABEL	DESCRIPTION
Rx fragments	This field shows the number of frames received that were less than 64 octets long, and contained an invalid FCS, including non-integral and integral lengths.
Rx error overrun	This field shows how many times an Ethernet transmitter overrun occurred.
Rx error mru	This field shows the number of received frames that were dropped due to exceeding the Maximum Receive Unit frame size.
Rx dropped	This field shows the number of received frames that were received into the IP DSLAM, but later dropped because of a lack of system resources.
Rx jabber	This field shows the number of frames received that were longer than 1518 octets (non VLAN) or 1522 octets (VLAN) and contained an invalid FCS, including alignment errors.
Rx error alignment	This field shows the number of frames received that were 64 to 1518 (non VLAN) or 1522 (VLAN) octets long but contained an invalid FCS and a non-integral number of octets.
Rx oversize	This field shows the number of frames received that were bigger than 1518 (non VLAN) or 1522 (VLAN) octets and contained a valid FCS.
Rx undersize	This field shows the number of frames received that were less than 64 octets long and contained a valid FCS.
Tx bytes	This field shows the number of bytes that have been transmitted on this port. This includes collisions but not jam signal or preamble/SFD (Start of Frame Delimiter) bytes.
Tx packets	This field shows the number of packets transmitted on this port.
Tx multicast	This field shows the number of good multicast frames transmitted on this port (not including broadcast frames).
Tx broadcast	This field shows the number of broadcast frames transmitted on this port (not including multicast frames).
Tx mac_pause	This field shows the number of valid IEEE 802.3x Pause frames transmitted on this port.
Tx fragments	This field shows the number of transmitted frames that were less than 64 octets long, and with an incorrect FCS value.
Tx frames	This field shows the number of complete good frames transmitted on this port.
Tx error underrun	This field shows the number of outgoing frames that were less than 64 octets long.
Tx undersize	This field shows the number of frames transmitted that were less than 64 octets long and contained a valid FCS.
Tx jabber	This field shows the number of frames transmitted that were longer than 1518 octets (non VLAN) or 1522 octets (VLAN) and contained an incorrect FCS value.
Tx oversize	This field shows the number of frames transmitted that were bigger than 1518 octets (non VLAN) or 1522 (VLAN) and contained a valid FCS.
packet(<=64)	This field shows the number of frames received and transmitted (including bad frames) that were 64 octets or less in length (this includes FCS octets but excludes framing bits).
packet(65-127)	This field shows the number of frames received and transmitted (including bad frames) that were 65 to 127 octets in length (this includes FCS octets but excludes framing bits).
packet(128-255)	This field shows the number of frames received and transmitted (including bad frames) that were 128 to 255 octets in length (this includes FCS octets but excludes framing bits).

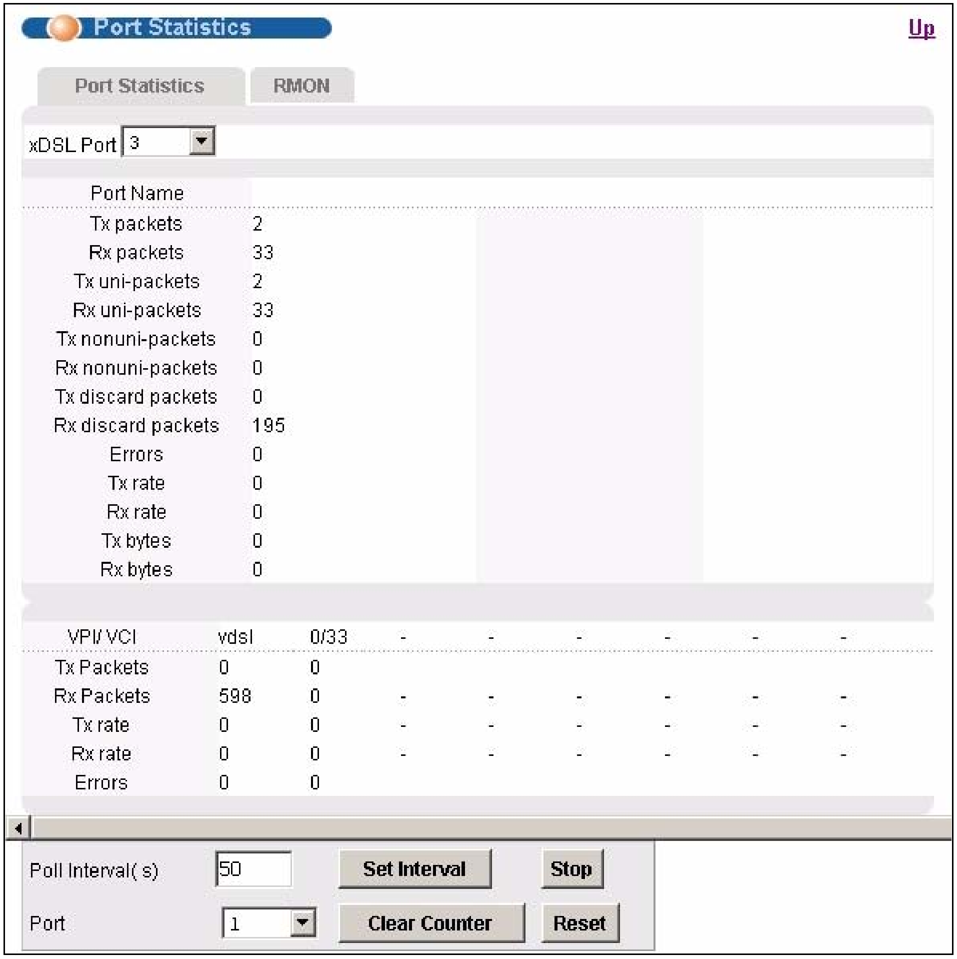
Table 6 Port Statistics (Ethernet) (continued)

LABEL	DESCRIPTION
packet(256-511)	This field shows the number of frames received and transmitted (including bad frames) that were 256 to 511 octets in length (this includes FCS octets but excludes framing bits).
packet(512-1023)	This field shows the number of frames received and transmitted (including bad frames) that were 512 to 1023 octets in length (this includes FCS octets but excludes framing bits).
packet(1024-1518)	This field shows the number of frames received and transmitted (including bad frames) that were 1024 to 1518 octets in length (this includes FCS octets but excludes framing bits).
packet(1522)	This field shows the number of frames received and transmitted (including bad frames) that were 1519 to 1522 octets in length (this includes FCS octets but excludes framing bits).
packet(total)	This field shows the total number of received and transmitted packets.
broadcast(total)	This field shows the total number of received and transmitted broadcast frames.
multicast(total)	This field shows the total number of received and transmitted multicast frames.
octet(total)	This field shows the total number of received and transmitted octets (unicast, multicast and broadcast).
Poll Interval(s) Set Interval	The text box displays how often (in seconds) this screen refreshes. You may change the refresh interval by typing a new number in the text box and then clicking **Set Interval**.
Stop	Click **Stop** to halt system statistic polling.
Port Clear Counter	Select a port from the **Port** drop-down list box and then click **Clear Counter** to erase the recorded statistical information for that port.
Reset	Click this to set the **Poll Interval(s)** and **Port** fields to their default values and to refresh the screen.

9.1.2 VDSL Port Statistics Screen

Use this screen to display statistics about a VDSL port. To open this screen, click a VDSL port’s number in the **Home** screen.

Figure 35 Port Statistics (VDSL)



xDSL Port 3

Port Name	
Tx packets	2
Rx packets	33
Tx uni-packets	2
Rx uni-packets	33
Tx nonuni-packets	0
Rx nonuni-packets	0
Tx discard packets	0
Rx discard packets	195
Errors	0
Tx rate	0
Rx rate	0
Tx bytes	0
Rx bytes	0

VPI/ VCI	vdsl	0/33	-	-	-	-	-	-
Tx Packets	0	0						
Rx Packets	598	0	-	-	-	-	-	-
Tx rate	0	0	-	-	-	-	-	-
Rx rate	0	0	-	-	-	-	-	-
Errors	0	0						

Poll Interval(s) 50

Port 1

The following table describes the labels in this screen.

Table 7 Port Statistics (VDSL)

LABEL	DESCRIPTION
Up	Click this to go back to the **Home** screen.
xDSL Port	Use this drop-down list box to select a port for which you wish to view statistics. This field identifies the port described in this screen.
Port Name	This field displays the name that you have configured for the port. If you have not configured a name, it is blank.
Tx packets	This field shows the number of packets transmitted on this port.
Rx packets	This field shows the number of packets received on this port.
Tx uni-packets	This field shows the number of unicast packets transmitted on this port.
Rx uni-packets	This field shows the number of unicast packets received on this port.
Tx nonuni-packets	This field shows the number of non unicast packets transmitted on this port.
Rx nonuni-packets	This field shows the number of non unicast packets received on this port.
Tx discard packets	This field shows the number of outgoing packets that were dropped on this port. The “Tx discard packets” counter always displays “0” because the IP DSLAM does not discard packets that it sends.

Table 7 Port Statistics (VDSL) (continued)

LABEL	DESCRIPTION
Rx discard packets	This field shows the number of received packets that were dropped on this port. Some of the possible reasons for the discarding of received (rx) packets are: • The packet filter is enabled and the packets matched a packet filter. • The MAC filter is enabled and the IP DSLAM dropped the packets according to the MAC filter's configuration. • The packets contained frames with an invalid VLAN ID.
Errors	This field shows the number of AAL5 frames received with CRC errors.
Tx rate	This field shows the number of kilobytes per second transmitted on this port.
Rx rate	This field shows the number of kilobytes per second received on this port.
Tx bytes	This field shows the number of bytes that have been transmitted on this port.
Rx bytes	This field shows the number of bytes that have been received on this port.
VPI/VCI	This field displays the Virtual Path Identifier (VPI) and Virtual Circuit Identifier (VCI) of channels on this port. **vdsl** displays when a VDSL device connects to this port.
Tx Packets	This field shows the number of packets transmitted on each channel.
Rx Packets	This field shows the number of packets received on each channel.
Tx rate	This field shows the number of bytes per second transmitted on each channel.
Rx rate	This field shows the number of bytes per second received on each channel.
Errors	This field shows the number of error packets on each channel.
Poll Interval(s) Set Interval	The text box displays how often (in seconds) this screen refreshes. You may change the refresh interval by typing a new number in the text box and then clicking **Set Interval**.
Stop	Click **Stop** to halt system statistic polling.
Port Clear Counter	Select a port from the **Port** drop-down list box and then click **Clear Counter** to erase the recorded statistical information for that port.
Reset	Click this to set the **Poll Interval(s)** and **Port** fields to their default values and to refresh the screen.

System Information

The **System Information** screen displays general device information (such as firmware version number) and hardware polling information (such as fan status). You can check the firmware version number and monitor the hardware status in this screen.

To open this screen, click **Basic Setting** > **System Information**.

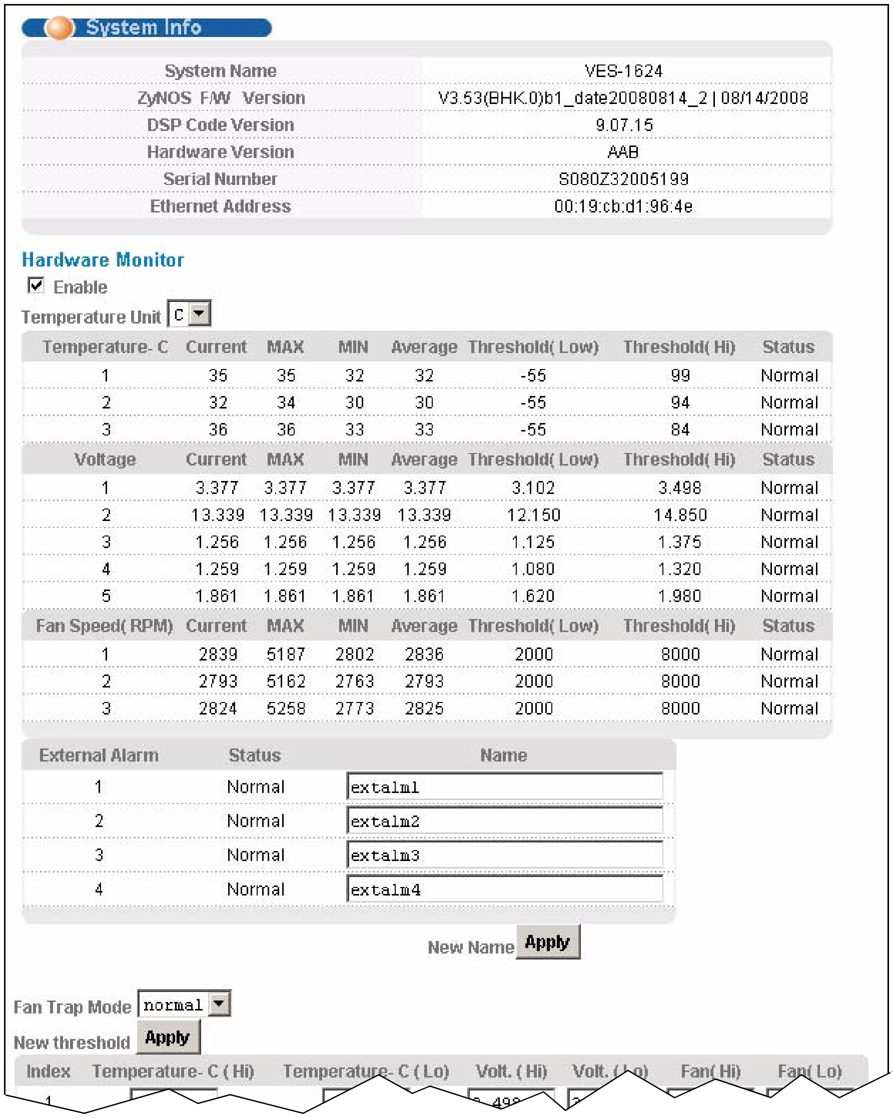


Figure 36 System Info

System Name	VES-1624
ZyNOS F/W Version	V3.53(BHK.0)b1_date20080814_2 | 08/14/2008
DSP Code Version	9.07.15
Hardware Version	AAB
Serial Number	S080Z32005199
Ethernet Address	00:19:cb:d1:96:4e

Hardware Monitor

☑ Enable

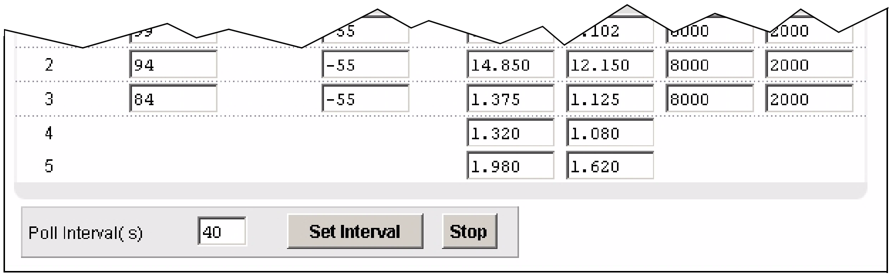
Temperature Unit C

Temperature- C	Current	MAX	MIN	Average	Threshold(Low)	Threshold(Hi)	Status
1	35	35	32	32	-55	99	Normal
2	32	34	30	30	-55	94	Normal
3	36	36	33	33	-55	84	Normal
Voltage	**Current**	**MAX**	**MIN**	**Average**	**Threshold(Low)**	**Threshold(Hi)**	**Status**
1	3.377	3.377	3.377	3.377	3.102	3.498	Normal
2	13.339	13.339	13.339	13.339	12.150	14.850	Normal
3	1.256	1.256	1.256	1.256	1.125	1.375	Normal
4	1.259	1.259	1.259	1.259	1.080	1.320	Normal
5	1.861	1.861	1.861	1.861	1.620	1.980	Normal
Fan Speed(RPM)	**Current**	**MAX**	**MIN**	**Average**	**Threshold(Low)**	**Threshold(Hi)**	**Status**
1	2839	5187	2802	2836	2000	8000	Normal
2	2793	5162	2763	2793	2000	8000	Normal
3	2824	5258	2773	2825	2000	8000	Normal

External Alarm	Status	Name
1	Normal	extalm1
2	Normal	extalm2
3	Normal	extalm3
4	Normal	extalm4

Fan Trap Mode normal

Index	Temperature- C (Hi)	Temperature- C (Lo)	Volt. (Hi)	Volt. (Lo)	Fan(Hi)	Fan(Lo)



2	94	-55	14.850	12.150	8000	2000
3	84	-55	1.375	1.125	8000	2000
4			1.320	1.080		
5			1.980	1.620		

Poll Interval(s) 40

The following table describes the labels in this screen.

Table 8 System Info

LABEL	DESCRIPTION
System Name	This field displays the device 's model name.
Software F/W Version	This field displays the version number of the device's current firmware including the date created.
DSP Code Version	This field displays the current Digital Signal Processor firmware version number. This is the modem code firmware.
Hardware Version	This is the version of the physical device hardware.
Serial Number	This is the individual identification number assigned to the device at the factory.
Ethernet Address	This field refers to the Ethernet MAC (Media Access Control) address of the device.
Hardware Monitor	
Enable	Select this check box to turn the hardware monitor on or clear it to turn the hardware monitor off.
Temperature Unit	Select **C** to display all temperature measurements in degrees Celsius. Select **F** to display all temperature measurements in degrees Fahrenheit.
Temperature- C	Each temperature sensor can detect and report the temperature. Temperature sensor 1 is near the DSL chipset. Temperature sensor 2 is near the central processing unit. Temperature sensor 3 is at the hardware monitor chip.
Current	This shows the current temperature at this sensor.
MAX	This field displays the maximum temperature measured at this sensor.
MIN	This field displays the minimum temperature measured at this sensor.
Average	This field displays the average temperature measured at this sensor.
Threshold (Low)	This field displays the lowest temperature limit at this sensor.
Threshold (Hi)	This field displays the highest temperature limit at this sensor.
Status	This field displays **Normal** for temperatures below the threshold and **Over** for those above.
Voltage	The power supply for each voltage has a sensor that can detect and report the voltage.
Current	This is the current voltage reading.
MAX	This field displays the maximum voltage measured at this point.
MIN	This field displays the minimum voltage measured at this point.
Average	This field displays the average voltage measured at this sensor.
Threshold (Low)	This field displays the lowest voltage limit at this sensor.
Threshold (Hi)	This field displays the highest voltage limit at this sensor.

Table 8 System Info (continued)

LABEL	DESCRIPTION
Status	**Normal** indicates that the voltage is within an acceptable operating range at this point; otherwise **Abnormal** is displayed.
Fan Speed (RPM)	A properly functioning fan is an essential component (along with a sufficiently ventilated, cool operating environment) in order for the device to stay within the temperature threshold. Each fan has a sensor that can detect and report the fan's RPM (Revolutions Per Minute).
Current	This is the current RPM reading.
MAX	This field displays the maximum RPM measured at this point.
MIN	This field displays the minimum RPM measured at this point.
Average	This field displays the average RPM measured at this sensor.
Threshold (Low)	This field displays the lowest RPM limit at this sensor.
Threshold (Hi)	This field displays the highest RPM limit at this sensor.
Status	**Normal** indicates that the RPM is within an acceptable operating range at this point; otherwise **Abnormal** is displayed.
External Alarm Status Name Apply	The IP DSLAM is able to detect alarm input from other equipment connected to the **ALARM** connector. The **Status** column displays **Normal** when no alarm input has been detected from other equipment. It displays **Abnormal** when alarm input has been detected from other equipment. Use the **Name** column to configure a title for each external alarm for identification purposes. Use up to 31 characters. Click **Apply** to save the name changes to the IP DSLAM's volatile memory. The IP DSLAM loses these changes if it is turned off or loses power, so use the **Config Save** link on the navigation panel to save your changes to the non-volatile memory when you are done configuring.
Fan Trap Mode	The IP DSLAM has three fans. Select **normal** to have the IP DSLAM send an SNMP trap if either one of the fans fails to function well. Select **two** to have the IP DSLAM send an SNMP trap only when more than one of the fans fail.
	Use this section below to configure the hardware monitor threshold settings.
New threshold Apply	Configure new threshold settings in the fields below and click **Apply** to use them.
Index	This field is a sequential value.
Temperature- C (Hi)	Use these fields to configure the highest temperature limit at each sensor.
Temperature- C (Lo)	Use these fields to configure the lowest temperature limit at each sensor.
Volt. (Hi)	Use these fields to configure the highest voltage limit at each sensor.
Volt. (Lo)	Use these fields to configure the lowest voltage limit at each sensor.
Fan (Hi)	Use these fields to configure the highest RPM limit at each sensor.
Fan (Low)	Use these fields to configure the lowest RPM limit at each sensor.
Poll Interval(s) Set Interval	The text box displays how often (in seconds) this screen refreshes. You may change the refresh interval by typing a new number in the text box and then clicking **Set Interval**.
Stop	Click **Stop** to halt statistic polling.

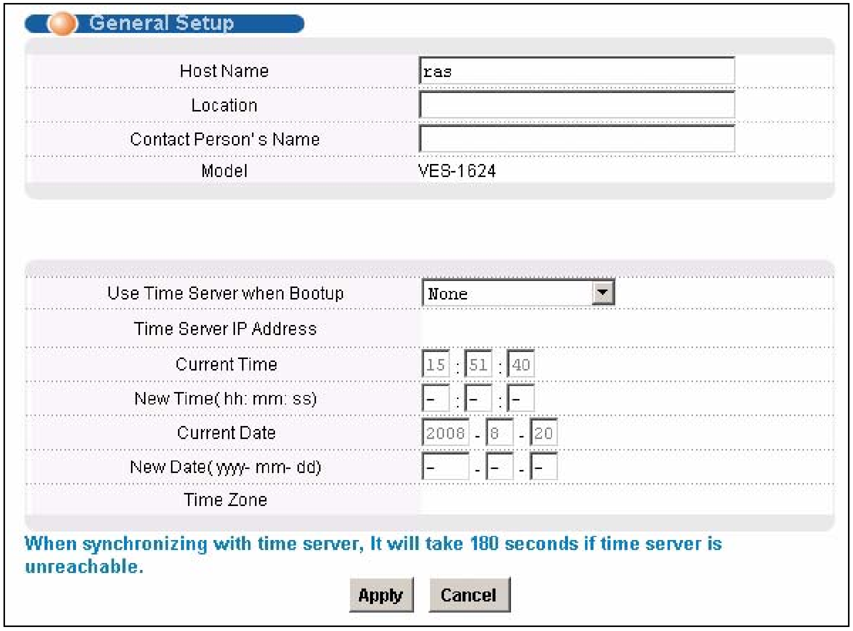
11

General Setup

The **General Setup** screen allows you to configure general device identification information. It also allows you to set the system time manually or get the current time and date from an external server when you turn on your device. The real time is then displayed in the logs.

To open this screen, click **Basic Setting** > **General Setup**.

Figure 37 General Setup



General Setup

Host Name	ras
Location	
Contact Person' s Name	
Model	VES-1624

Use Time Server when Bootup	None
Time Server IP Address	
Current Time	15 : 51 : 40
New Time(hh: mm: ss)	- : - : -
Current Date	2008 - 8 - 20
New Date(yyyy- mm- dd)	- - - - -
Time Zone	

When synchronizing with time server, It will take 180 seconds if time server is unreachable.

The following table describes the labels in this screen.

Table 9 General Setup

LABEL	DESCRIPTION
Host Name	Choose a descriptive name for identification purposes. This name consists of up to 31 ASCII characters; spaces are not allowed.
Location	Enter the geographic location of your device. You can use up to 31 ASCII characters; spaces are not allowed.
Contact Person's Name	Enter the name of the person in charge of this device. You can use up to 31 ASCII characters; spaces are not allowed.
Model	This field displays your device type.

Table 9 General Setup (continued)

LABEL	DESCRIPTION
Use Time Server When Bootup	Select the time service protocol that the timeserver uses. Not all time servers support all protocols, so you may have to use trial and error to find a protocol that works. The main differences between them are the time format. When you select the **Daytime (RFC 867)** format, the IP DSLAM displays the day, month, year and time with no time zone adjustment. When you use this format it is recommended that you use a Daytime timeserver within your geographical time zone. **Time (RFC-868)** format displays a 4-byte integer giving the total number of seconds since 1970/1/1 at 0:0:0. **NTP (RFC-1305)** is similar to Time (RFC-868). **None** is the default value. Enter the time manually. Each time you turn on the device, the time and date will be reset to 2000-1-1 0:0.
Time Server IP Address	Enter the IP address of your timeserver. The device searches for the timeserver for up to 60 seconds. Click **Sync** if you want to get the IP DSLAM time updated with the time server you specified immediately. This field is available when you selected **Daytime (RFC 867)**, **Time (RFC-868)** or **NTP (RFC-1305)** in the **Use Time Server When Bootup** field.
Current Time	This field displays the time you open this menu (or refresh the menu).
New Time (hh:mm:ss)	Enter the new time in hour, minute and second format. The new time then appears in the **Current Time** field after you click **Apply**.
Current Date	This field displays the date you open this menu.
New Date (yyyy-mm-dd)	Enter the new date in year, month and day format. The new date then appears in the **Current Date** field after you click **Apply**.
Time Zone	Select the time difference between UTC (Universal Time Coordinated, formerly known as GMT, Greenwich Mean Time) and your time zone from the drop-down list box. This field is only available when you selected **Time (RFC-868)** or **NTP (RFC-1305)** in the **Use Time Server When Bootup** field.
Apply	Click **Apply** to save your changes to the IP DSLAM's volatile memory. The IP DSLAM loses these changes if it is turned off or loses power, so use the **Config Save** link on the navigation panel to save your changes to the non-volatile memory when you are done configuring.
Cancel	Click **Cancel** to start configuring the screen again.

12

User Account

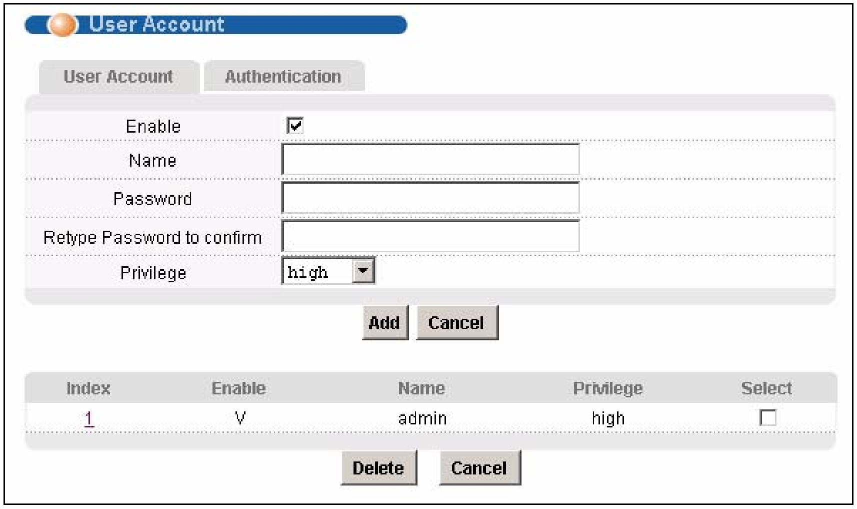
The **User Account** screens allows you to set up and configure system administrator accounts for the IP DSLAM. You can also configure the authentication policy for IP DSLAM administrators. This is different than port authentication in Chapter 27 on page 167.

See Chapter 27 on page 167 for background information on authentication.

12.1 User Account Screen

To open this screen, click **Basic Setting** > **User Account**.

Figure 38 User Account



Enable	☑
Name	
Password	
Retype Password to confirm	
Privilege	high

Index	Enable	Name	Privilege	Select
1	V	admin	high	□

The following table describes the labels in this screen.

Table 10 User Account

LABEL	DESCRIPTION
Enable	Select this check box to turn on the administrator account.
Name	Enter a user name for the administrator account.
Password	Enter a password for the administrator account.
Retype Password to confirm	Re-enter the administrator account's password to verify that you have entered it correctly.

Table 10 User Account (continued)

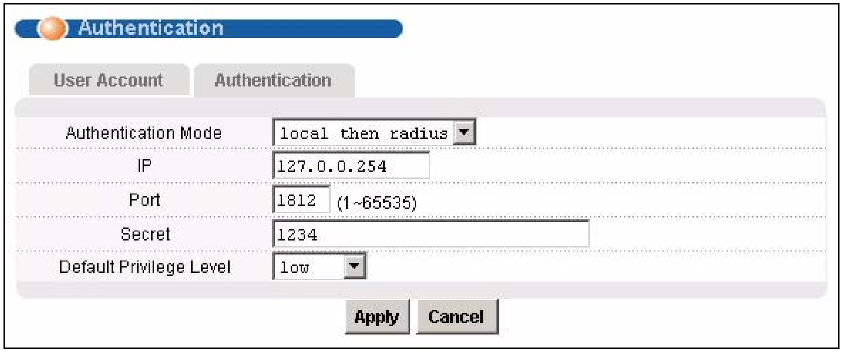
LABEL	DESCRIPTION
Privilege	Select a privilege level to determine which screens the administrator can use. There is a high, medium or low privilege level for each command. Select **high** to allow the administrator to use all commands including the lower privilege commands. High privilege commands include things like creating administrator accounts, restarting the system and resetting the factory defaults. Select **middle** to allow the administrator to use middle or low privilege commands. Select **low** to allow the administrator to use only low privilege commands. Low privilege commands are read only.
Add	Click **Add** to save your changes to the IP DSLAM's volatile memory. The IP DSLAM loses these changes if it is turned off or loses power, so use the **Config Save** link on the navigation panel to save your changes to the non-volatile memory when you are done configuring.
Cancel	Click **Cancel** to begin configuring the fields again.
Index	This field displays the number of the user account. Click an account's index number to use the top of the screen to edit it.
Enable	This field displays a "**V** " if you have the administrator account turned on. It displays a "**-**" if the administrator account is turned off.
Name	This field displays the administrator account's user name.
Privilege	This field displays the administrator account's access level (**high**, **middle** or **low**).
Select	Select this check box and click the **Delete** button to remove an administrator account.
Delete	Select an administrator account's check box and click this button to remove the administrator account.
Cancel	Click **Cancel** to start configuring the screen afresh.

12.2 Authentication Screen

Use this screen to set up the authentication policies and settings by which administrators can access the IP DSLAM.

To open this screen, click **Basic Setting** > **User Account** > **Authentication**.

Figure 39 Authentication



Authentication Mode	local then radius
IP	127.0.0.254
Port	1812 (1~65535)
Secret	1234
Default Privilege Level	low

The following table describes the labels in this screen.

Table 11 Authentication

LABEL	DESCRIPTION
Authentication Mode	Select the process by which the IP DSLAM authenticates administrators. **local** - Search the local database. You maintain this database in the **User Account** screen. **radius** - Check an external RADIUS database using the settings below. **local then radius** - Search the local database; if the user name is not found, check an external RADIUS database using the settings below.
IP	Enter the IP address of the external RADIUS server in dotted decimal notation.
Port	The default UDP port of the RADIUS server for authentication is **1812**. You need not change this value unless your network administrator instructs you to do so.
Secret	Specify a password (up to 31 alphanumeric characters) as the key to be shared between the external RADIUS server and the IP DSLAM. This key is not sent over the network. This key must be the same on the external RADIUS server and the IP DSLAM.
Default Privilege Level	Select the privilege level assigned to administrators in case the external RADIUS database does not provide one. The privilege level determines which screens the administrator can use. There is a high, medium or low privilege level for each command. You can also choose to deny access to the IP DSLAM. Select **high** to allow the administrator to use all commands including the lower privilege commands. High privilege commands include things like creating administrator accounts, restarting the system and resetting the factory defaults. Select **middle** to allow the administrator to use middle or low privilege commands. Select **low** to allow the administrator to use only low privilege commands. Low privilege commands are read only. Select **deny** to prevent the administrator from accessing the IP DSLAM.

13

Switch Setup

The **Switch Setup** screen allows you to set up and configure global device features.

13.1 Switch Modes

The IP DSLAM supports daisychain and aggregation switch modes.

13.1.1 Daisychain Switch Mode

Daisychain switch mode sets the IP DSLAM to use Ethernet port one (ENET 1) as an uplink port to connect to the Ethernet backbone and Ethernet port two (ENET 2) to connect to another (daisychained or subtending) IP DSLAM. When you daisychain multiple IP DSLAM they must all be set to daisychain mode.

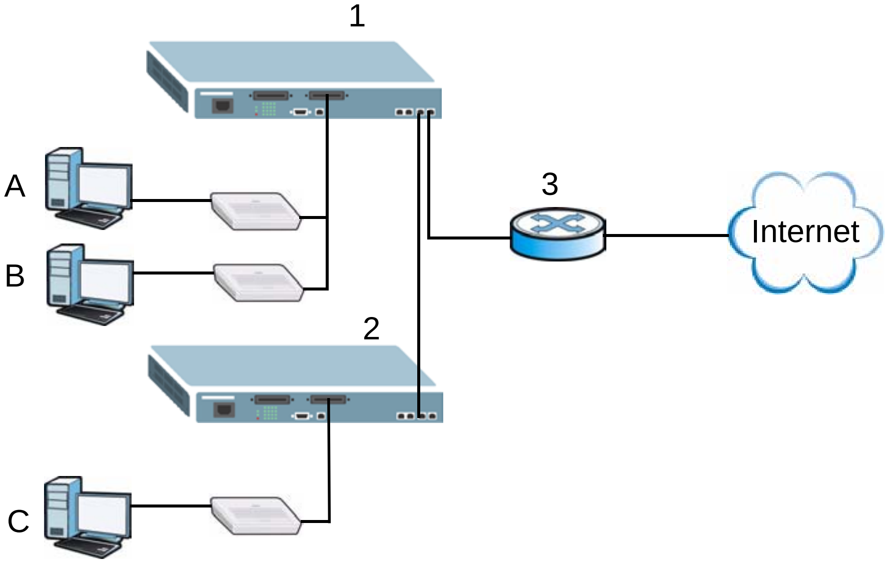
Daisychain switch mode with port isolation enabled blocks communications between subscriber ports on an individual IP DSLAM and between the subscribers of any daisychained IP DSLAM (see Figure 40 on page 92 for an example). Use the same port isolation setting on all IP DSLAM that you set up in a daisychain.

13.1.2 Port Isolation with Daisychain Switch Mode Example

In the example below, the IP DSLAM 1 has its Ethernet port one (ENET 1) connected to the Ethernet backbone switch (**3**) and it’s Ethernet port two (ENET2) connected to Ethernet port one (ENET 1) of the daisychained IP DSLAM (**2**).

With port isolation turned on, communications between **A** and **B** must first go through another switch or router (**3** in the figure). **A** and **B** also cannot communicate with **C** without their communications going through another switch or router.

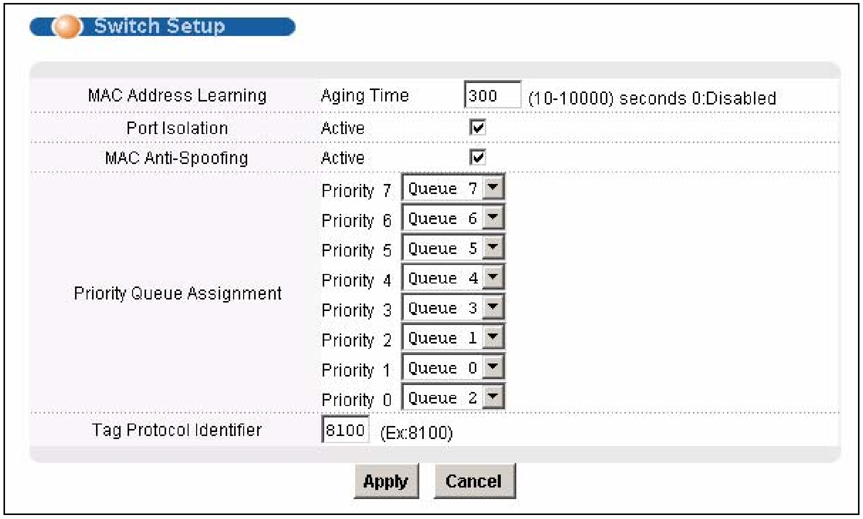
Figure 40 Port Isolation with Daisychain Switch Mode Example



13.2 Switch Setup Screen

To open this screen, click **Basic Setting** > **Switch Setup**.

Figure 41 Switch Setup



MAC Address Learning	Aging Time	300 (10-10000) seconds 0:Disabled
Port Isolation	Active	☑
MAC Anti-Spoofing	Active	☑
Priority Queue Assignment	Priority 7	Queue 7
	Priority 6	Queue 6
	Priority 5	Queue 5
	Priority 4	Queue 4
	Priority 3	Queue 3
	Priority 2	Queue 1
	Priority 1	Queue 0
	Priority 0	Queue 2
Tag Protocol Identifier	8100 (Ex:8100)	

The following table describes the labels in this screen.

Table 12 Switch Setup

LABEL	DESCRIPTION
MAC Address Learning Aging Time	Enter a time from 10 to 10,000 seconds. This is how long all dynamically learned MAC addresses remain in the MAC address table before they age out (and must be relearned). Enter 0 to disable the aging out of MAC addresses.
Port Isolation Active	Select this to turn on port isolation to block communications between subscriber ports. When you enable port isolation, you do not need to configure the VLAN to isolate subscribers. When you clear this, the **VLAN Isolation** link appears. See Section 13.2 on page 92.

Table 12 Switch Setup (continued)

LABEL	DESCRIPTION
MAC Anti-Spoofing	Select this to have the IP DSLAM detect whether a MAC address is connected to more than one port.
Priority Queue Assignment	IEEE 802.1p defines up to 8 separate traffic types by inserting a tag into a MAC-layer frame that contains bits to define class of service. Frames without an explicit priority tag are given the default priority of the ingress port. Use the next two fields to configure the priority level-to-physical queue mapping.
Priority 7	Typically used for network control traffic such as router configuration messages.
Priority 6	Typically used for voice traffic that is especially sensitive to jitter (jitter is the variations in delay).
Priority 5	Typically used for video that consumes high bandwidth and is sensitive to jitter.
Priority 4	Typically used for controlled load, latency-sensitive traffic such as SNA (Systems Network Architecture) transactions.
Priority 3	Typically used for “excellent effort” or better than best effort and would include important business traffic that can tolerate some delay.
Priority 2	This is for “spare bandwidth”.
Priority 1	This is typically used for non-critical “background” traffic such as bulk transfers that are allowed but that should not affect other applications and users.
Priority 0	Typically used for best-effort traffic.
Tag Protocol Identifier	Enter a 4-digit protocol ID which is added together with VLAN (including priority) tag on traffic. By default, it is 8100 which means Ethernet traffic. This also has the IP DSLAM accept tagged traffic with the same protocol ID, but drop tagged traffic with a different protocol ID.
Apply	Click **Apply** to save your changes to the IP DSLAM’s volatile memory. The IP DSLAM loses these changes if it is turned off or loses power, so use the **Config Save** link on the navigation panel to save your changes to the non-volatile memory when you are done configuring.
Cancel	Click **Cancel** to begin configuring this screen afresh.

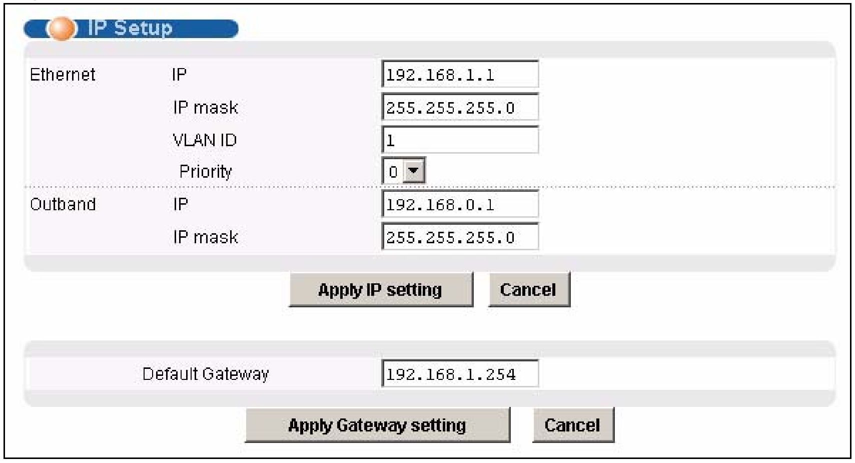
14

IP Setup

The **IP Setup** screen allows you to configure a device IP address, subnet mask and DNS (domain name server) for management purposes.

To open this screen, click **Basic Setting** > **IP Setup**.

Figure 42 IP Setup



IP Setup

Ethernet	IP	192.168.1.1
	IP mask	255.255.255.0
	VLAN ID	1
	Priority	0
Outband	IP	192.168.0.1
	IP mask	255.255.255.0

Default Gateway 192.168.1.254

The following table describes the labels in this screen.

Table 13 IP Setup

LABEL	DESCRIPTION
Ethernet	This section allows you to configure the IP setup for your IP DSLAM management through in-band ports.
IP	Enter the IP address for management of your IP DSLAM in dotted decimal notation for example 1.2.3.4.
IP mask	Enter the IP subnet mask for management of your IP DSLAM in dotted decimal notation (for example, 255.255.255.0).
VLAN ID	This is the VLAN ID for your IP DSLAM management. See Chapter 19 on page 133 for more information on configuring VLANs on the IP DSLAM.
Priority	This is the priority level for your IP DSLAM management. "0" is the lowest priority level and "7" is the highest.
Outband	This section allows you to configure the IP settings for the IP DSLAM management through the **MGMT** port.
IP	Enter the IP address for management of your IP DSLAM in dotted decimal notation for example 1.2.3.4.
IP mask	Enter the IP subnet mask for management of your IP DSLAM in dotted decimal notation (for example, 255.255.255.0).
Apply IP setting	

Table 13 IP Setup (continued)

LABEL	DESCRIPTION
Cancel	Click **Cancel** to begin configuring the above fields again.
Default Gateway	Enter the IP address of the default outgoing gateway for the in-band network (in dotted decimal notation).
Apply Gateway setting	Click **Apply Gateway setting** to save your changes to the IP DSLAM's volatile memory. The IP DSLAM loses these changes if it is turned off or loses power, so use the **Config Save** link on the navigation panel to save your changes to the non-volatile memory when you are done configuring.
Cancel	Click **Cancel** to begin configuring the default gateway field again.

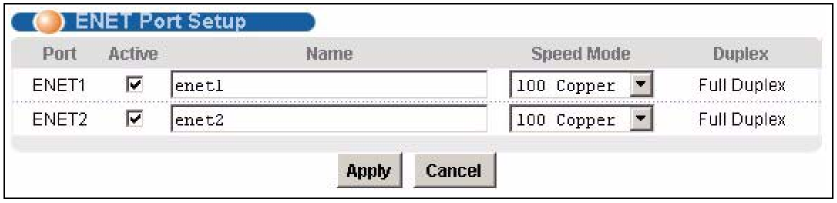
15

ENET Port Setup

The **ENET Port Setup** screen allows you to configure settings for the Ethernet ports.

To open this screen, click **Basic Setting** > **ENET Port Setup**.

Figure 43 ENET Port Setup



Port	Active	Name	Speed Mode	Duplex
ENET1	☑	enet1	100 Copper	Full Duplex
ENET2	☑	enet2	100 Copper	Full Duplex

The following table describes the labels in this screen.

Table 14 ENET Port Setup

LABEL	DESCRIPTION
Port	This is the port index number.
Active	Select the check box to turn on the port. Clear it to disable the port.
Name	Enter a descriptive name that identifies this port. You can use up to 31 ASCII characters; spaces are not allowed.
Speed Mode	Select the type of Ethernet connection for this port. When you don't use auto-negotiation, you must make sure that the settings of the peer Ethernet port are the same in order to connect. Select **Auto** (auto-negotiation) to have the IP DSLAM automatically determine the type of connection that the Ethernet port has. When the peer Ethernet device has auto-negotiation turned on, the IP DSLAM negotiates with the peer to determine the connection speed. If the peer Ethernet port does not have auto-negotiation turned on, the IP DSLAM determines the connection speed by detecting the signal on the cable and using full duplex. When an Ethernet port is set to **Auto**, the IP DSLAM tries to make a fiber connection first and does not attempt to use the RJ-45 port if the fiber connection is successful. Select **100 Copper** if the Ethernet port has a 100 MB electrical connection. Select **1000 Copper** if the Ethernet port has a 1000 MB (1 gigabit) electrical connection. Select **1000 Fiber** if the Ethernet port has a 1000 MB (1 gigabit) fiber optic connection.
Duplex	The IP DSLAM uses full duplex Ethernet connections.
Apply	Click **Apply** to save your changes to the IP DSLAM's volatile memory. The IP DSLAM loses these changes if it is turned off or loses power, so use the **Config Save** link on the navigation panel to save your changes to the non-volatile memory when you are done configuring.
Cancel	Click **Cancel** to begin configuring this screen afresh.

16

xDSL Port Setup

This chapter explains how to configure settings for profiles and individual DSL ports. It also covers how to configure virtual channels and virtual channel profiles.

16.1 DSL Profiles

A DSL profile is a table that contains a list of pre-configured DSL settings. Each DSL port has one (and only one) profile assigned to it at any given time. You can configure multiple profiles, including profiles for troubleshooting. Profiles allow you to configure DSL ports efficiently. You can configure many DSL ports with the same profile, thus removing the need to configure the settings of each DSL port one-by-one. You can also change an individual DSL port’s settings by assigning it a different profile.

For example, you could set up different profiles for different kinds of accounts (for example, economy, standard and premium). Assign the appropriate profile to a DSL port and it takes care of a large part of the port’s configuration. You still get to individually enable or disable each port, as well as configure its channels and operational mode. See the chapter on profiles for how to configure DSL profiles.

16.2 Alarm Profiles

Alarm profiles define DSL port alarm thresholds. The system sends an alarm trap and generates a syslog entry when the thresholds of the alarm profile are exceeded. See the chapter on profiles for how to configure alarm profiles.

16.3 Interleave Delay

Interleave delay is the wait (in milliseconds) that determines the size of a single block of data to be interleaved (assembled) and then transmitted. Interleave delay is used when transmission error correction (Reed-Solomon) is necessary due to a less than ideal telephone line. The bigger the delay, the bigger the data block size, allowing better error correction to be performed.

Reed-Solomon codes are block-based error correcting codes with a wide range of applications. The Reed-Solomon encoder takes a block of digital data and adds extra "redundant" bits. The Reed-Solomon decoder processes each block and attempts to correct errors and recover the original data.

16.3.1 Fast Mode

Fast mode means no interleaving takes place and transmission is faster (a “fast channel”). This would be suitable if you have a good line where little error correction is necessary.

16.4 VDSL Parameters

The following sections describe the VDSL parameters you configure in the following screens:

- xDSL Port Setup (see Section 16.9 on page 105).
- xDSL Port Profile (see Section 17.1 on page 117).

16.4.1 PSD

PSD (Power Spectral Density) defines the distribution of a VDSL line’s power in the frequency domain. A PSD mask specifies the maximum allowable PSD for a line.

16.4.2 Limit PSD Mask

To reduce the impact of interference and attenuation, ITU-T 993.2 specifies a limit PSD mask that limits the VDSL2 transmitters PSD at both downstream and upstream.

16.4.3 RFI (Radio Frequency Interference)

RFI is induced noise on the lines by surrounding radio frequency electromagnetic radiation from sources such as AM and HAM radio stations. Since VDSL uses a much larger frequency range that overlaps with other radio frequency systems, signals from VDSL lines and other radio systems interfere with each other. To avoid performance degradation due to RFI, set the switch to not transmit VDSL signals in the RFI band defined by the regulatory bodies (ETSI and ANSI). You can also configure your own RFI bands on the system.

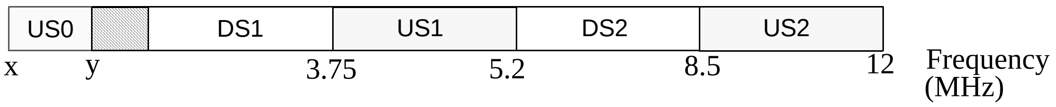
16.4.4 Frequency Band Plan

Each VDSL mode operates in a different frequency band allocation, resulting in different upstream and downstream speeds. Your Device automatically changes the band plan based on the loop condition and loop length.

A band plan example is shown next. Band plans include an optional band (between 25 kHz and 276 kHz) controlled by "limit PSD mask".

The optional band is used for upstream transmission which is to be negotiated during line initiation. The optional band frequency (for example, the positions of **x** and **y** in the following figure) varies depending on the limit PSD mask you use.

Figure 44 A Band Plan Example



The sample of optional band PSD mask and associated frequency band used in the Device is shown next.

Table 15 Optional band PSD Mask

LIMIT PSD MASK		OPTIONAL BAND FREQUENCY
nus0_d32	=	No optional band
eu32_d32	=	25 ~ 138 kHz
eu36_d48	=	25 ~ 155.25 kHz
. . .		

The "eu" number in the limit PSD mask is a tone index. A tone spacing, 4.3125 KHz, is used for VDSL2 profile from 8a up to 17a. So "eu32" means the optional band ending at around 138 kHz. See more information in Section 16.4.5 on page 101.

16.4.5 VDSL2 Profiles

ITU-T G993.2 defines eight VDSL2 profiles (8a, 8b, 8c, 8d, 12a, 12b, 17a, and 30a) based on each annex specifying spectral characters (Annexes A, B and C).

Note: At the time of writing, the IP DSLAM supports the Annex A with 8a, 8b, 8c, 8d, 12a, 12b, and 17a. The following table summarizes the VDSL2 profiles supported by the IP DSLAM.

Table 16 VDSL2 Profiles In The Device

FREQUENCY PLAN	PARAMETER	PARAMETER VALUE FOR PROFILES						
		8a	8b	8c	8d	12a	12b	17a
Annex A	Maximum aggregate downstream transmit power (dBm)	+17.5	+20.5	+11.5	+14.5	+14.5	+14.5	+14.5
	Index of highest supported downstream data-bearing sub-carrier (upper band edge frequency in MHz (informative))	1971 (8.5)	1971 (8.5)	1971 (8.5)	1971 (8.5)	1971 (8.5)	1971 (8.5)	4095 (17.660)
	Index of highest supported upstream data-bearing sub-carrier (upper band edge frequency in MHz (informative))	1205 (5.2)	1205 (5.2)	1205 (5.2)	1205 (5.2)	2782 (12)	2782 (12)	2782 (12)

16.4.6 Impulse Noise Protection (INP)

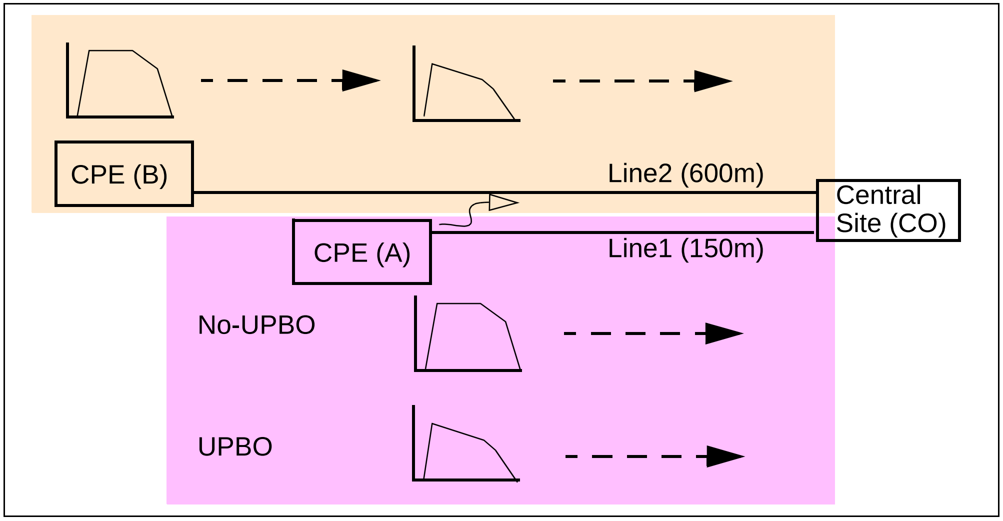
Short impulses from external sources may cause bursts of errors which could impact the multimedia (ex. voice, video, or picture) quality. VDSL2 supports Impulse Noise Protection (INP) which provides the ability to correct errors regardless of the number of errors in an errored DMT (Discrete Multi-Tone) symbol.

16.4.7 UPBO

In a network with varying telephone wiring lengths, the PSD on each line is different. This causes crosstalk between the lines. Enable UPBO (Upstream Power Back Off) to allow the device to adjust the transmit PSD of all lines based on a reference line length. This mitigates the upstream crosstalk on shorter loops to longer loops. It allows the IP DSLAM to provide better service in a network environment with telephone wiring of varying lengths.

An example is shown below. **Line 1** and **Line 2** are in the same cable binder. Crosstalk occurs when the signal flows and is near to **CPE (A)**'s location. Besides, higher **Line 1** PSD causes higher interference to the **Line 2**. **CO** receives signal with higher attenuation. With UPBO enabled on the **CPE (A)**, it decreases the PSD level and reduces the crosstalk impact on long loops.

Figure 45 UPBO Resolves Upstream Far-End Crosstalk



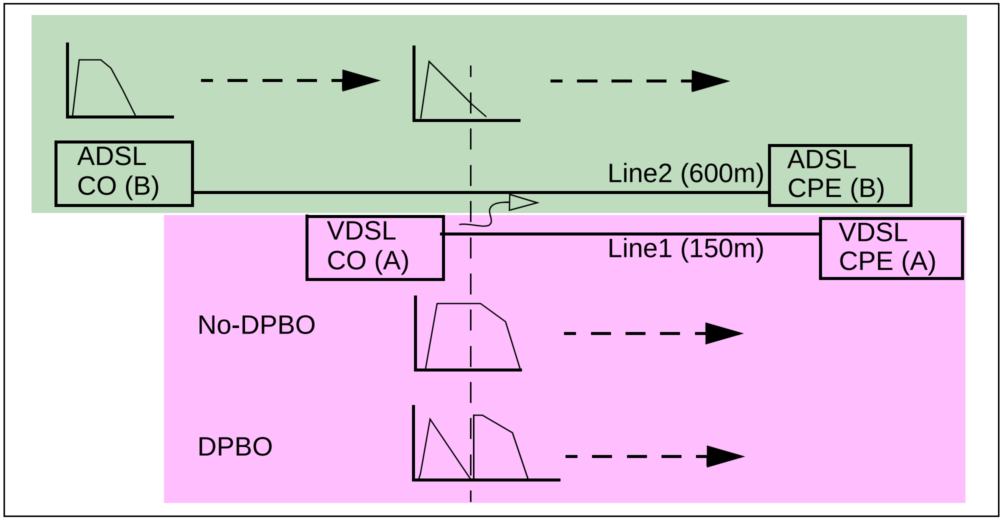
16.4.8 DPBO

VDSL signal may interfere with other services (such as ISDN, ADSL or ADSL2 provided by other devices) on the same bundle of lines due to downstream far-end crosstalk. DPBO (Downstream Power Back Off) can reduce performance degradation by changing the PSD level on the VDSL device(es) at street cabinet level.

ISDN in Europe uses a frequency range of up to 80 kHz, while ISDN in Japan uses a frequency range of up to 640 kHz. ADSL utilizes the 1.1 MHz band. Both ADSL2 and ADSL 2+ utilize the 2.2 MHz band.

An example is shown next. VDSL **Line 1** and ADSL **Line 2** are in the same binder. Crosstalk occurs when the ADSL signal flows from **CO (B)** and is near to **CO (A)**'s ONU (Optical Network Unit) location. Besides, higher **Line 1** PSD causes higher interference to the **Line 2**. **CPE (B)** receives signal with higher attenuation. With DPBO enabled on the **CO (A)**, it decreases the PSD level and reduces the crosstalk impact on other service lines.

Figure 46 DPBO Resolves Downstream Far-End Crosstalk



16.4.9 DPBO Electrical Length

The distance between a cabinet and the central office is an important parameter of DPBO settings as we mentioned in the Section 16.4.8 on page 102. The electrical length is used instead of the real physical distance according to G.997.1 format. Depending on the cable type the line used and physical line length, you can calculate the electrical length (in dB). For example, the distance is 1 kilometer and you use 24 AWG cable type, the electrical length 20.5 dB is suggested to used.

The following table displays the calculation from a real length to an electrical length.

Table 17 Real Length to Electrical Length

CABLE TYPE	REAL LENGTH TO ELECTRICAL LENGTH	A	B	C
22 AWG	=16.2*(cable length in kilometer)	0	0	0
24 AWG	=20.5*(cable length in kilometer)	0	1	0
26 AWG	=25.8*(cable length in kilometer)	0	1.0039065	-0.0039065

16.5 DSL Standards Overview

These are the DSL standards and rates that the IP DSLAM supports at the time of writing. The actual transfer rates will vary depending on what the subscriber's device supports, the line conditions and the connection distance.

Table 18 DSL Standards Maximum Transfer Rates

STANDARD	MAXIMUM DOWNSTREAM	MAXIMUM UPSTREAM
8a/b/c/d	85 Mbps	18 Mbps
12a/b	85 Mbps	50 Mbps
17a	100 Mbps	50 Mbps
ADSL2+	24 Mbps	1 Mbps

16.6 Downstream and Upstream

Downstream refers to traffic going out from the IP DSLAM to the subscriber's DSL modem or router. Upstream refers to traffic coming into the IP DSLAM from the subscriber's DSL modem or router.

16.7 Configured Versus Actual Rate

You configure the maximum rate of an individual DSL port by modifying its profile (see Chapter 17 on page 117) or assigning the port to a different profile (see Section 16.9.1 on page 106). However, due to noise and other factors on the line, the actual rate may not reach the maximum that you specify.

Even though you can specify arbitrary numbers using the Edit Profile screen, the actual rate is always a multiple of 32 Kbps. If you enter a rate that is not a multiple of 32 Kbps, the actual rate will be the next lower multiple of 32Kbps. For instance, if you specify 60 Kbps for a port, the actual rate for that port will not exceed 32 Kbps, and if you specify 66 Kbps, the actual rate will not be over 64Kbps.

Regardless of a profile's configured upstream and downstream rates, the IP DSLAM automatically limits the actual rates for each individual port to the maximum speeds supported by the port's DSL operational mode. For example, if you configure a profile with a maximum downstream rate of 25000 Kbps, and apply it to a port set to use G.dmt, the IP DSLAM automatically uses a maximum downstream rate of 8160 Kbps. This means that if you configure a profile with very high rates, you can still use it with any port. See Table 18 on page 104 for a list of the maximum rates supported by the different xDSL standards.

16.8 Default Settings

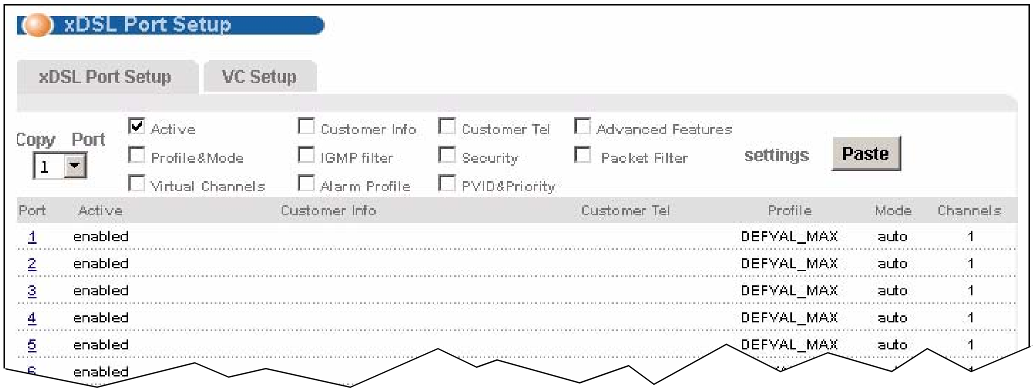
The default profile always exists and all of the DSL ports use the default profile settings when the IP DSLAM is shipped. The default profile's name is set to `DEFVAL_MAX`.

See Chapter 54 on page 283 for the settings of the default profile and DSL port default settings.

16.9 xDSL Port Setup Screen

To open this screen, click **Basic Setting** > **xDSL Port Setup**.

Figure 47 xDSL Port Setup



xDSL Port Setup

xDSL Port Setup | VC Setup

Copy Port [1 ▼]

☑ Active □ Customer Info □ Customer Tel □ Advanced Features
□ Profile&Mode □ IGMP filter □ Security □ Packet Filter settings Paste
□ Virtual Channels □ Alarm Profile □ PVID&Priority

Port	Active	Customer Info	Customer Tel	Profile	Mode	Channels
1	enabled			DEFVAL_MAX	auto	1
2	enabled			DEFVAL_MAX	auto	1
3	enabled			DEFVAL_MAX	auto	1
4	enabled			DEFVAL_MAX	auto	1
5	enabled			DEFVAL_MAX	auto	1
6	enabled					

The following table describes the labels in this screen.

Table 19 xDSL Port Setup

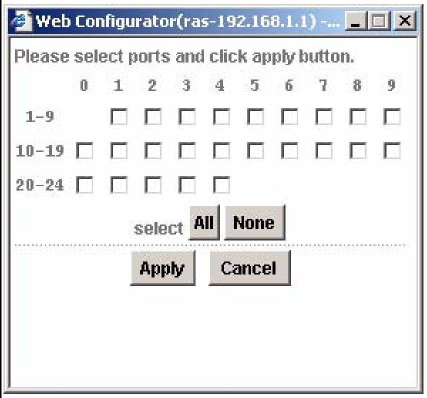
LABEL	DESCRIPTION
Copy Port Paste	Do the following to copy settings from one DSL port to another DSL port or ports. 1. Select the number of the DSL port from which you want to copy settings. 2. Select the settings that you want to copy. 3. Click **Paste** and the following screen appears. 4. Select to which ports you want to copy the settings. Use **All** to select every port. Use **None** to clear all of the check boxes. 5. Click **Apply** to paste the settings. **Figure 48** Select Ports  Web Configurator(ras-192.168.1.1) -... Please select ports and click apply button. 0 1 2 3 4 5 6 7 8 9 1-9 □ □ □ □ □ □ □ □ □ 10-19 □ □ □ □ □ □ □ □ □ □ 20-24 □ □ □ □ □ select All None Apply Cancel
Active	Select this check box to copy this port's active setting. This is configured in the **xDSL Port Setting** screen (see Section 16.9.1 on page 106).
Customer Info	Select this check box to copy this port's subscriber information. This is configured in the **xDSL Port Setting** screen (see Section 16.9.1 on page 106).
Customer Tel	Select this check box to copy this port's subscriber's telephone number. This is configured in the **xDSL Port Setting** screen (see Section 16.9.1 on page 106).
Advanced Features	Select this check box to copy this port's VDSL feature settings. These are configured in the **xDSL Port Setting** screen (see Section 16.9.1 on page 106).

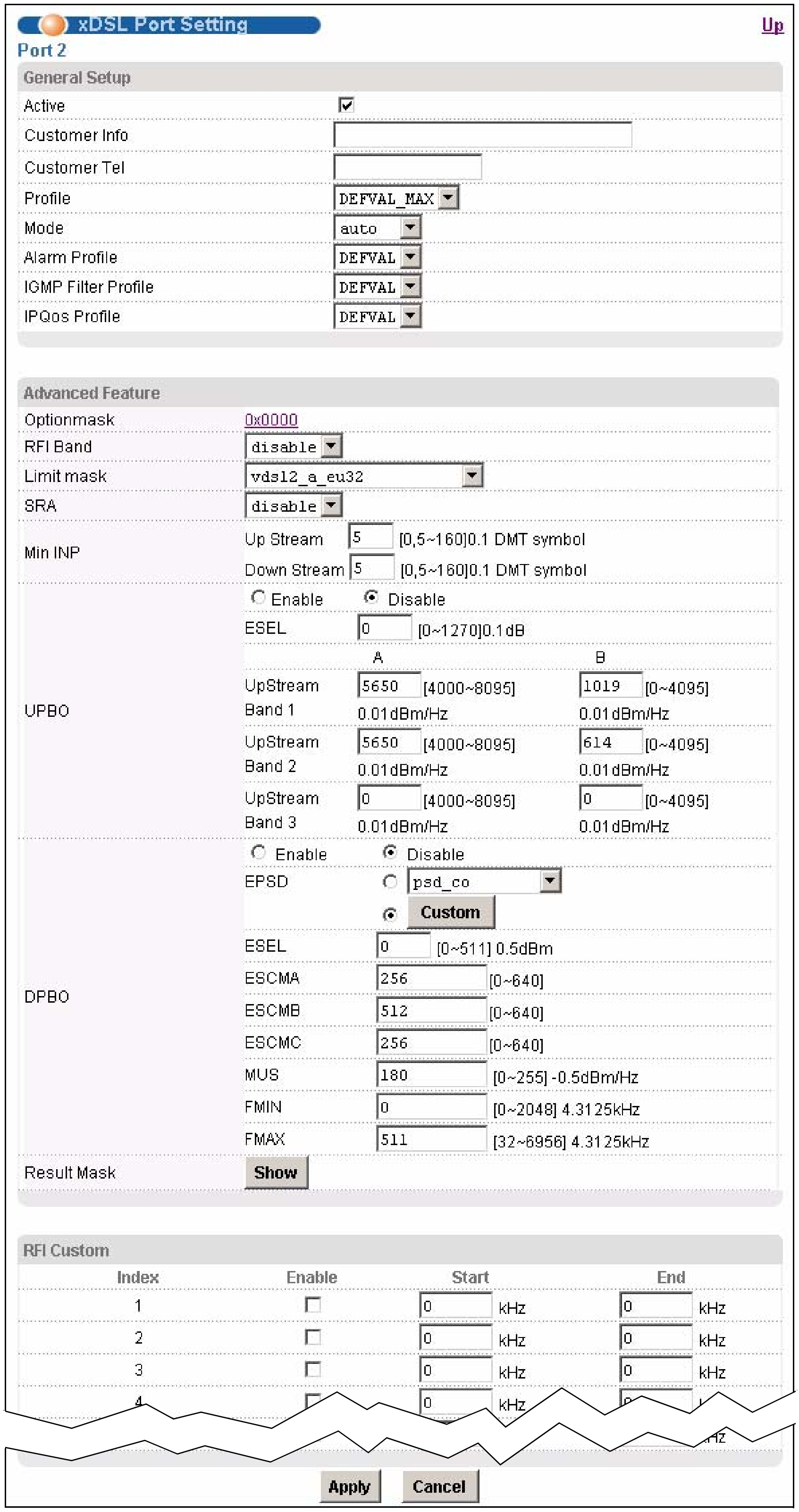
Table 19 xDSL Port Setup (continued)

LABEL	DESCRIPTION
Profile&Mode	Select this check box to copy this port's port profile settings and DSL operational mode. The port profile settings are configured in the **xDSL Profiles Setup** screens (see Chapter 17 on page 117). The DSL operational mode is configured in the **xDSL Port Setting** screen (see Section 16.9.1 on page 106).
IGMP filter	Select this check box to copy this port's IGMP filter settings. These are configured in the **IGMP Filter Profile** screen (see Section 21.7 on page 147).
Security	Select this check box to copy this port's security settings. This is configured in the **Port Security** screen (see Section 28.2 on page 171).
Packet Filter	Select this check box to copy this port's packet filter settings. These are configured in the **Packet Filtering** screen (see Section 24.1 on page 157).
Virtual Channels	Select this check box to copy this port's virtual channel settings. These are configured in the **VC Setup** screen (see Section 16.11 on page 113).
Alarm Profile	Select this check box to copy this port's alarm profile. This is configured in the **Alarm Profile Setup** screen (see Section 17.3 on page 121).
PVID&Priority	Select this check box to copy this port's PVID and priority settings. These are configured in the **VLAN Port Setting** screen (see Section 19.5 on page 137).
Paste	See **Copy Port**.
Port	This field shows each xDSL port number.
Active	This field shows the active status of this port. The port may be **enabled** or **disabled**. This is configured in the **xDSL Port Setting** screen (see Section 16.9.1 on page 106).
Customer Info	This field shows the customer information provided for this port. This is configured in the **xDSL Port Setting** screen (see Section 16.9.1 on page 106).
Customer Tel	This field shows the customer telephone number provided for this port. This is configured in the **xDSL Port Setting** screen (see Section 16.9.1 on page 106).
Profile	This field shows which profile is assigned to this port. This is configured in the **xDSL Port Setting** screen (see Section 16.9.1 on page 106).
Mode	This field shows which DSL operational mode the port is set to use. This is configured in the **xDSL Port Setting** screen (see Section 16.9.1 on page 106).
Channels	This field displays the number of PVCs (Permanent Virtual Circuits) that are configured for this port. This is configured in the **VC Setup** screen (see Section 16.11 on page 113).

16.9.1 xDSL Port Setting Screen

To open this screen, click **Basic Setting** > **xDSL Port Setup**, and then click a port's index number.

Figure 49 xDSL Port Setting



Port 2

General Setup

Active	☑
Customer Info	
Customer Tel	
Profile	DEFVAL_MAX
Mode	auto
Alarm Profile	DEFVAL
IGMP Filter Profile	DEFVAL
IPQos Profile	DEFVAL

Advanced Feature

Optionmask	0x0000				
RFI Band	disable				
Limit mask	vdsl2_a_eu32				
SRA	disable				
Min INP	Up Stream	5	[0,5~160]0.1 DMT symbol		
	Down Stream	5	[0,5~160]0.1 DMT symbol		
UPBO	○ Enable	● Disable			
	ESEL	0	[0~1270]0.1dB		
		A		B	
	UpStream Band 1	5650	[4000~8095] 0.01dBm/Hz	1019	[0~4095] 0.01dBm/Hz
	UpStream Band 2	5650	[4000~8095] 0.01dBm/Hz	614	[0~4095] 0.01dBm/Hz
	UpStream Band 3	0	[4000~8095] 0.01dBm/Hz	0	[0~4095] 0.01dBm/Hz
DPBO	○ Enable	● Disable			
	EPSD	○ psd_co ● Custom			
	ESEL	0	[0~511] 0.5dBm		
	ESCMA	256	[0~640]		
	ESCMB	512	[0~640]		
	ESCMC	256	[0~640]		
	MUS	180	[0~255] -0.5dBm/Hz		
	FMIN	0	[0~2048] 4.3125kHz		
	FMAX	511	[32~6956] 4.3125kHz		
Result Mask	Show				

RFI Custom

Index	Enable	Start	End
1	□	0 kHz	0 kHz
2	□	0 kHz	0 kHz
3	□	0 kHz	0 kHz
4	□	0 kHz	

The following table describes the labels in this screen.

Table 20 xDSL Port Setting

LABEL	DESCRIPTION
Up	Click this to return to the previous screen.
General Setup	
Active	Select this check box to turn on this DSL port.
Customer Info	Enter information to identify the subscriber connected to this DSL port. You can use up to 31 printable ASCII characters (including spaces and hyphens).
Customer Tel	Enter information to identify the telephone number of the subscriber connected to this DSL port. You can use up to 15 ASCII characters (including spaces and hyphens).
Profile	Select a profile of DSL settings (such as the transfer rate, interleave delay and signal to noise ratio settings) to assign to this port. Use the **Port Profile** screen to configure port profiles (see Chapter 17 on page 117).
Mode	Select the port's DSL operational mode. Select the mode that the subscriber's device uses or **auto** to have the IP DSLAM automatically determine the mode to use. See Table 22 on page 114 for information on the individual DSL modes.
Alarm Profile	Select the port's alarm profile. The alarm profile defines alarm thresholds for the DSL port. The IP DSLAM sends an alarm trap and generates a syslog entry when the thresholds of the alarm profile are exceeded (see Section 17.3 on page 121).
IGMP Filter Profile	The IGMP filter profile defines which multicast groups a port can join. Select a profile of IGMP filter settings to assign to this port. Use the **IGMP Filter Profile** screen to configure IGMP filter profiles (see Section 21.7 on page 147).
IPQos Profile	Select an IPQoS profile to classify and prioritize application traffic.
Advanced Feature	

Table 20 xDSL Port Setting (continued)

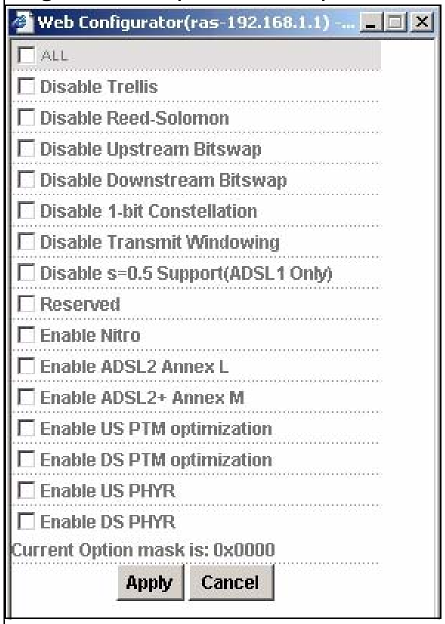
LABEL	DESCRIPTION
Optionmask	Click the link to display the following screen where you can configure the optional band PSD mask. 1. Select which setting(s) you want to apply to the option mask. Select **ALL** to select every setting and click it again to clear all of the check boxes. 2. See the configured result in the **Current Option mask is** field. 3. Click **Apply** to go back to the **xDSL Port Setting** screen. **Figure 50** Optionmask options  □ ALL □ Disable Trellis □ Disable Reed-Solomon □ Disable Upstream Bitswap □ Disable Downstream Bitswap □ Disable 1-bit Constellation □ Disable Transmit Windowing □ Disable s=0.5 Support(ADSL1 Only) □ Reserved □ Enable Nitro □ Enable ADSL2 Annex L □ Enable ADSL2+ Annex M □ Enable US PTM optimization □ Enable DS PTM optimization □ Enable US PHYR □ Enable DS PHYR Current Option mask is: 0x0000
RFI Band	RFI is induced noise on the lines by surrounding radio frequency electromagnetic radiation from sources such as AM and HAM radio stations. To avoid performance degradation due to RFI, set the IP DSLAM to not transmit VDSL signals in the RFI band defined by the regulatory bodies such as ETSI (**etsi**) or ANSI (**ansi**). You can also configure your own RFI bands on the system (**custom**) or **disable** it.
Limit mask	To reduce the impact of interference and attenuation on downstream and upstream transmissions, ITU-T 993.2 specifies a limit PSD mask that limits the VDSL2 transmitter's PSD. VDSL CPE devices refer to the limit PSD mask to adjust its PSD level when transmitting data. Select a PSD mask to specify the frequency distribution. From the mask list, you can also see the upstream and downstream bands. For example, select **vdsl2_a_nus0** to use upstream band 0 and up to its 32nd sub-carrier and downstream band 1 starting from the 32nd sub-carrier. Available options are listed as follows. vdsl2_a_nus0, vdsl2_a_eu32, vdsl2_a_eu36, vdsl2_a_eu40, vdsl2_a_eu44, vdsl2_a_eu48, vdsl2_a_eu52, vdsl2_a_eu56, vdsl2_a_eu60, vdsl2_a_eu64, vdsl2_a_eu128, vdsl1_fttex_ansi_m1, vdsl1_fttex_ansi_m2, vdsl1_fttcab_ansi_m1, vdsl1_fttcab_ansi_m2, vdsl1_fttex_ansi_m1_e, vdsl1_fttex_ansi_m2_e, vdsl1_fttcab_ansi_m1_e, vdsl1_fttcab_ansi_m2_e, vdsl2_a_ct, vdsl2_b8_1, vdsl2_b8_2, vdsl2_b8_3, vdsl2_b8_4, vdsl2_b8_5, vdsl2_b8_6, vdsl2_b8_7, vdsl2_b8_8, vdsl2_b8_9, vdsl2_b8_10, vdsl2_b8_11, vdsl2_b8_12, vdsl2_b8_13, vdsl2_b8_14, vdsl2_b8_15, vdsl2_b8_16, vdsl2_b7_1, vdsl2_b7_2, vdsl2_b7_3, vdsl2_b7_4, vdsl2_b7_5, vdsl2_b7_6, vdsl2_b7_7, vdsl2_b7_8, vdsl2_b7_9, vdsl2_b7_10, vdsl2_bt_anfp, vdsl2_c_138_b, vdsl2_c_276_b, vdsl2_c_138_co, vdsl2_c_276_co

Table 20 xDSL Port Setting (continued)

LABEL	DESCRIPTION
Min INP	Specify the level of impulse noise (burst) protection for a slow (or interleaved) channel related to upstream or downstream transmissions. This parameter is defined as the number of consecutive DMT symbols or fractions thereof. The number of symbols decides how long in one period errors can be completely corrected. A higher symbol value provides higher error correction capability, but it causes overhead and higher delay which may impact multimedia data receiving quality. Enter **0** to disable impulse noise protection.
UPBO	UPBO (Upstream Power Back-Off) mitigates far-end crosstalk (FEXT) caused by upstream transmission on shorter loops to longer loops. See Section 13.1.7 on page 169. Select **Enable** or **Disable** to turn it on or off.
ESEL	This is Upstream Power Back-off Exchange-Side Electrical Length. This specifies the electrical length of the cable between CPE and CO. Set this other than 0 (1~1270, in 0.1 dB) to force CPE devices to use the Device's electrical length value for UPBO adjustment. Set this to 0 to use a dynamic electrical length based on the result of the negotiation between the Device and CPE devices.
Upstream Band 1, 2, 3	Specify 4000~8095 (0.01 dBm/Hz) for parameter **A** which defines the original band shape. Specify 0~4095 (0.01 dBm/Hz) for parameter **B** which defines the power back-off degree. Parameter **A** and **B** are used for UPBO PSD mask calculation.
DPBO	Select **Enable** to avoid interference with other services (such as ISDN, ADSL or ADSL2 provided by other devices) on the same bundle of lines. ISDN in Europe uses a frequency range of up to 80 kHz, while ISDN in Japan uses a frequency range of up to 640 kHz. ADSL utilizes the 1.1 MHz band. Both ADSL2 and ADSL2+ utilize the 2.2 MHz band. Select **Disable** to turn it off.
EPSD	This is a pre-defined PSD mask to reduce interference with other services (for example, ADSL) in the same copper bundle. **psd_co**: Select this if the Device is deployed at the CO and you want it to use the full ADSL band. **psd_flat**: Select this to have the Device not use the ADSL band. **psd_cab_ansi**: Select this if the Device is deployed in a cabinet and has to coexist with other services in region A. **psd_cab_etsi**: Select this if the Device is deployed in a cabinet and has to coexist with other services in region B. **psd_exch_etsi**: Select this if the Device is deployed in an exchange and has to co-exist with other services in region B. **psd_exch_ansi**: Select this if the Device is deployed in an exchange and has to co-exist with other services in region A. Please refer to G.993.2 appendix for region A and B. Click **Custom** to display a screen where you can customize breakpoints and PSD level for the PSD mask. See Section 16.9.2 on page 111.
DPBOESEL	This is the electrical length of the cable between CO and Cabinet. See Section 13.1.9 on page 170.
ESCMA, ESCMB, ESCMC	These parameters define a cable model that is used to describe the frequency dependent loss of exchange-side cables.
MUS	This defines the assumed minimum usable received PSD mask (in dBm/Hz) for exchange based services, used to modify parameter DPBOFMAX defined below.

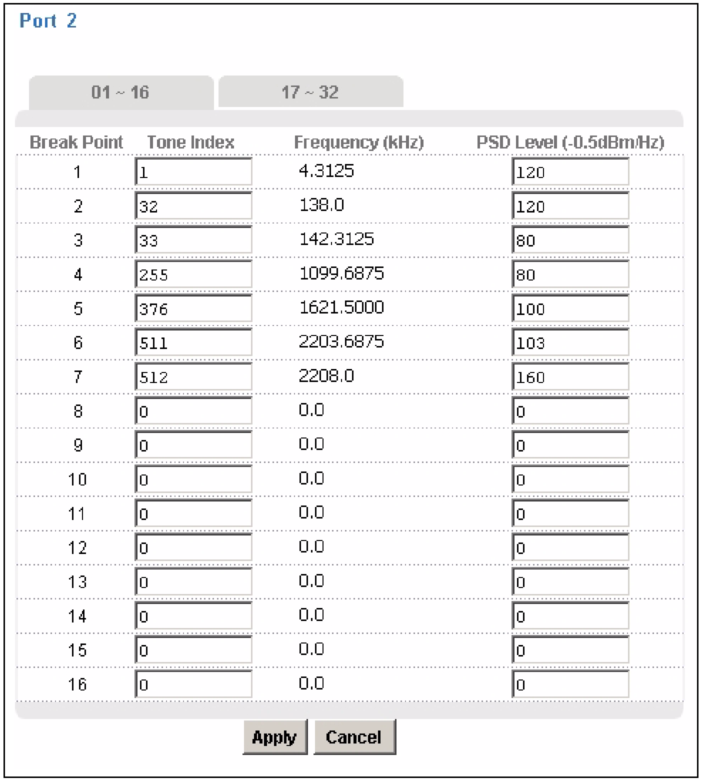
Table 20 xDSL Port Setting (continued)

LABEL	DESCRIPTION
FMIN	This defines the minimum frequency from which the DPBO shall be applied.
FMAX	This defines the maximum frequency at which DPBO may be applied.
Result Mask	Click **Show** to display the PSD mask result based on what you configured on this screen.
RFI Custom	Configure this section if you select **custom** in the **RFI Band** field above.
Index	This field displays the index number of an entry.
Enable	Select this to activate a custom RFI band.
Start	Specify the frequency a custom RFI band starts.
End	Specify the frequency a custom RFI band ends.
Apply	Click **Apply** to save your changes to the IP DSLAM's volatile memory. The IP DSLAM loses these changes if it is turned off or loses power, so use the **Config Save** link on the navigation panel to save your changes to the non-volatile memory when you are done configuring.
Cancel	Click **Cancel** to begin configuring the fields again.

16.9.2 DPBO EPSD: Custom

Click the **Custom** button in the **xDSL Port Setting** screen to open this screen. Your settings in this screen are one of the factors determining the PSD mask result.

Figure 51 DPBO EPSD: Custom



Port 2

Break Point	Tone Index	Frequency (kHz)	PSD Level (-0.5dBm/Hz)
1	1	4.3125	120
2	32	138.0	120
3	33	142.3125	80
4	255	1099.6875	80
5	376	1621.5000	100
6	511	2203.6875	103
7	512	2208.0	160
8	0	0.0	0
9	0	0.0	0
10	0	0.0	0
11	0	0.0	0
12	0	0.0	0
13	0	0.0	0
14	0	0.0	0
15	0	0.0	0
16	0	0.0	0

The following table describes the labels in this screen.

Table 21 DPBO EPSD: Custom

LABEL	DESCRIPTION
Port X	This field displays the port you are currently configuring.
01~16 17~32	Click the **01~16** tab to configure PSD levels for break points 1 to 16 and click the **17~32** tab to configure PSD levels for break points 17 to 32.
Break Point	This index number identifies each incremental break point. There are 32 break points in total you can configure.
Tone Index	A tone is a sub-channel of VDSL band. DMT divides VDSL bands into many 4.3125 kHz tones. Enter an increased number (than previous row) from 0 to 4096 in this field that is also the horizontal of the DPBOEPSD graph.
Frequency	This read-only field displays a frequency that equals the tone index multiple 4.3125 kHz. This field automatically calculates after a **Tone Index** value is entered.
PSD level	Enter the PSD level for the corresponding frequency break point.
Apply	Click **Apply** to save your changes back to the switch.
Cancel	Click **Cancel** to reload the previous configuration for this screen.

16.10 Virtual Channels

Defining virtual channels (also called Permanent Virtual Circuits or PVCs) allows you to set priorities for different services or subscribers. You can define up to eight channels on each DSL port and use them for different services or levels of service. You set the PVID that is assigned to untagged frames received on each channel. You also set an IEEE 802.1p priority for each of the PVIDs. In this way you can assign different priorities to different channels (and consequently the services that get carried on them or the subscribers that use them).

For example, you want to give high priority to voice service on one of the DSL ports.

Use the **Edit Static VLAN** screen to configure a static VLAN on the IP DSLAM for voice on the port.

Use the **DSL Edit Port Channel Setup** screen to:

- Configure a channel on the port for voice service.
- Set the channel to use the PVID of the static VLAN you configured.
- Assign the channel a high priority.

16.10.1 Super Channel

The IP DSLAM forwards frames belonging to VLAN groups that are not assigned to specific channels to the super channel. Enable the super channel option to allow a channel forward frames belonging to multiple VLAN groups (that are not assigned to other channels). The super channel functions in the same way as the channel in a single channel environment. One port can have only one super channel.

16.10.2 LLC

LLC is a type of encapsulation where one VC (Virtual Circuit) carries multiple protocols with each packet header containing protocol identifying information. Despite the extra bandwidth and processing overhead, this method may be advantageous if it is not practical to have a separate VC for each carried protocol, for example, if charging heavily depends on the number of simultaneous VCs.

16.10.3 VC Mux

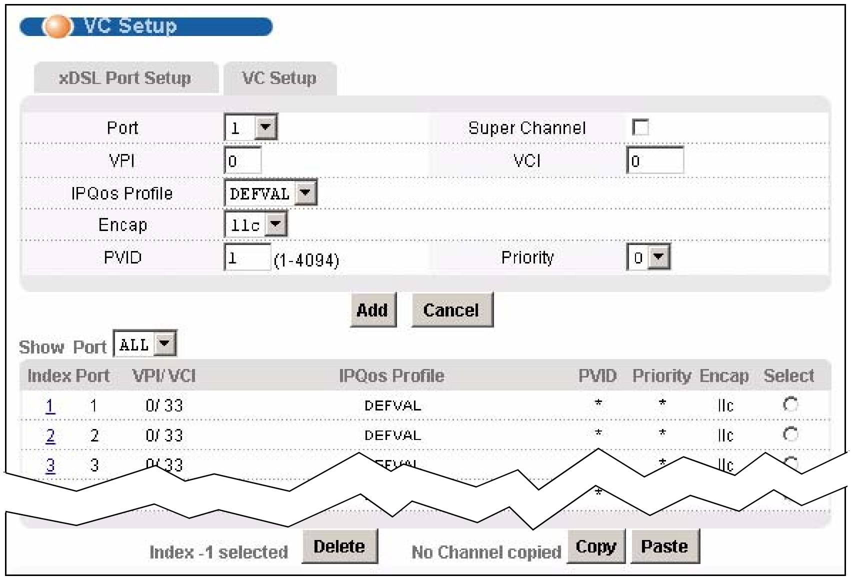
VC Mux is a type of encapsulation where, by prior mutual agreement, each protocol is assigned to a specific virtual circuit, for example, VC1 carries IP, VC2 carries IPX, and so on. VC-based multiplexing may be dominant in environments where dynamic creation of large numbers of ATM VCs is fast and economical.

16.11 VC Setup Screen

Use this screen to view and configure a port’s channel (PVC) settings.

To open this screen, click **Basic Setting** > **xDSL Port Setup** > **VC Setup**.

Figure 52 VC Setup



Port	1	Super Channel	□
VPI	0	VCI	0
IPQos Profile	DEFVAL		
Encap	llc		
PVID	1 (1-4094)	Priority	0

Show Port ALL

Index	Port	VPI/ VCI	IPQos Profile	PVID	Priority	Encap	Select
1	1	0/ 33	DEFVAL	*	*	llc	○
2	2	0/ 33	DEFVAL	*	*	llc	○
3	3	0/ 33	DEFVAL		*	llc	○
				*			

Index -1 selected

No Channel copied

The following table describes the labels in this screen.

Table 22 VC Setup

LABEL	DESCRIPTION
Port	Select a port for which you wish to view or configure settings. This field is read-only once you click on a port number below.
Super Channel	The IP DSLAM forwards frames belonging to VLAN groups that are not assigned to specific channels to the super channel. Enable the super channel option to have this channel forward frames belonging to multiple VLAN groups (that are not assigned to other channels). The super channel functions in the same way as the channel in a single channel environment.
VPI	Type the Virtual Path Identifier for a channel on this port.
VCI	Type the Virtual Circuit Identifier for a channel on this port.
IPQos Profile	Select an IPQoS profile to classify and prioritize application traffic. You can configure IPQoS profiles in the **Basic Settings** > **xDSL Profile Setup** > **IPQos Profile** screen (see Section 17.2 on page 119).
Encap	Select the encapsulation type (**llc** or **vc**) for this VC.
PVID	Type a PVID (Port VLAN ID) to assign to untagged frames received on this channel.
Priority	Use the drop-down list box to select the priority value (0 to 7) to add to incoming frames without a (IEEE 802.1p) priority tag. An asterisk (*) denotes a super channel.
Add/Apply	Click this to add or save channel settings on the selected port. (The name of the button depends on whether or not you have clicked on a VC number in the **Index** column.) This saves your changes to the IP DSLAM's volatile memory. The IP DSLAM loses these changes if it is turned off or loses power, so use the **Config Save** link on the navigation panel to save your changes to the non-volatile memory when you are done configuring.
Cancel	Click **Cancel** to start configuring the screen again.
Show Port	Select the number of an DSL port for which to display VC settings (or display all of them).
Index	This field displays the number of the VC. Click a VC's index number to use the top of the screen to edit the VC. Note: At the time of writing, you cannot edit the VPI and VCI. If you want to change them, add a new VC with the desired settings. Then you can delete any unwanted VCs.
Port	This field displays the number of the DSL port on which the VC is configured.
VPI/VCI	This field displays the Virtual Path Identifier (VPI) and Virtual Circuit Identifier (VCI). The VPI and VCI identify a channel on this port.
IPQos Profile	This filed displays an IPQoS profile applied on a port using this VC.
PVID	This is the PVID (Port VLAN ID) assigned to untagged frames or priority frames (0 VID) received on this channel. An asterisk (*) denotes a super channel.
Priority	This is the priority value (0 to 7) added to incoming frames without a (IEEE 802.1p) priority tag. An asterisk (*) denotes a super channel.
Encap	This field displays the encapsulation type (**llc** or **vc**) configured on a port for the VC.

Table 22 VC Setup (continued)

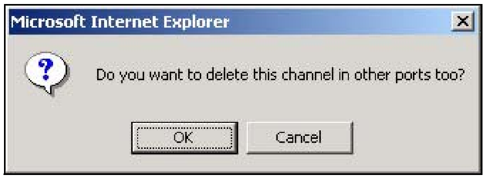
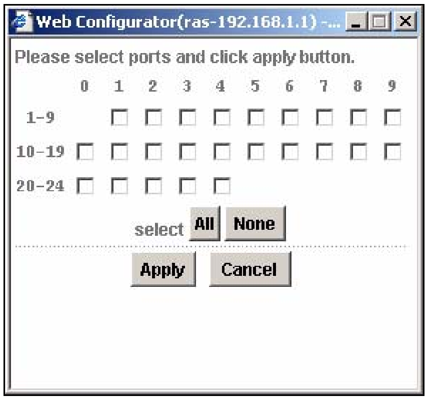
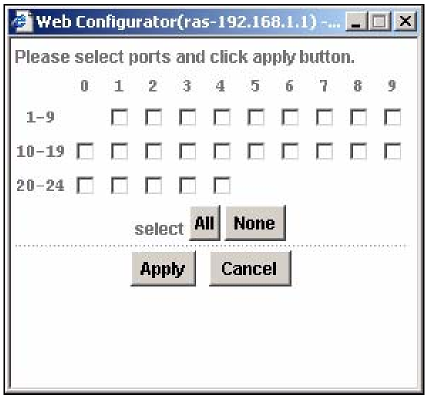
LABEL	DESCRIPTION
Select Delete	Do the following to remove one or more PVCs. 1. Select a PVC's **Select** radio button. 2. Click **Delete**. 3. Click **OK** if you want to remove the PVC from other ports. Click **Cancel** to only remove the one you selected. **Figure 53** Basic Setting > xDSL Port Setup > VC Setup > Delete  Microsoft Internet Explorer Do you want to delete this channel in other ports too? 4. If you clicked **OK**, the following screen appears. 5. Select to which ports you want to copy the settings. Use **All** to select every port. Use **None** to clear all of the check boxes. 6. Click **Apply** to delete the channels. **Figure 54** Select Ports  Web Configurator(ras-192.168.1.1) -... Please select ports and click apply button. 0 1 2 3 4 5 6 7 8 9 1-9 □ □ □ □ □ □ □ □ □ 10-19 □ □ □ □ □ □ □ □ □ □ 20-24 □ □ □ □ □

Table 22 VC Setup (continued)

LABEL	DESCRIPTION
Select Copy Paste	Do the following to copy settings from one PVC to another port or ports. 1. Click the **Select** radio button of the PVC from which you want to copy settings. 2. Click **Paste**. 3. The following screen appears. 4. Select to which ports you want to copy the settings. Use **All** to select every port. Use **None** to clear all of the check boxes. 5. Click **Apply** to copy the settings. **Figure 55** Select Ports  Please select ports and click apply button. Web Configurator(ras-192.168.1.1) -... 0 1 2 3 4 5 6 7 8 9 1-9 □ □ □ □ □ □ □ □ □ 10-19 □ □ □ □ □ □ □ □ □ □ 20-24 □ □ □ □ □ select All None Apply Cancel

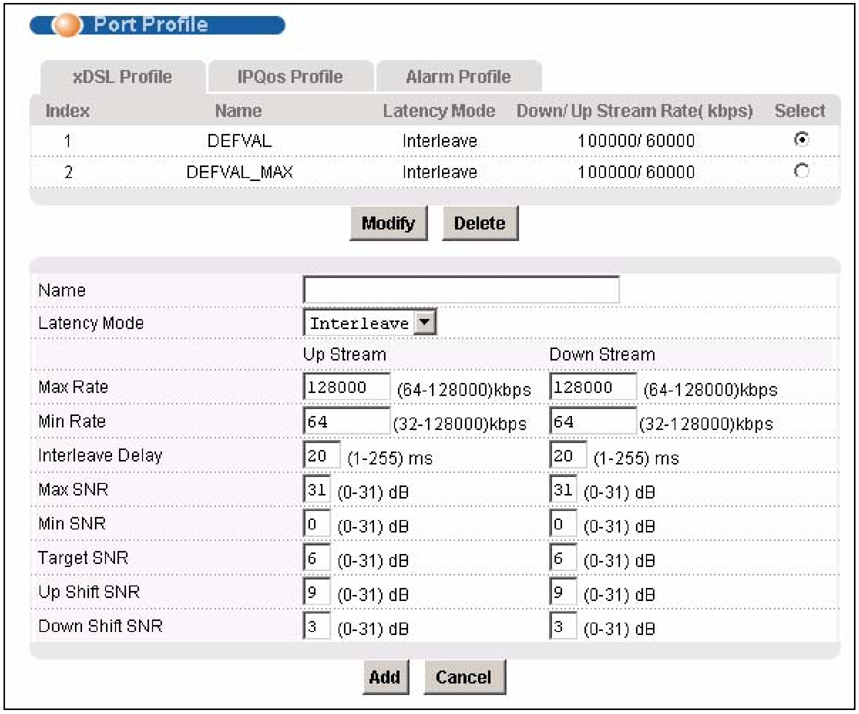
xDSL Profiles Setup

A profile is a list of settings that you define. Then you can assign them to one or more individual ports. For background information about many of these settings, see Chapter 16 on page 99.

17.1 xDSL Port Profile Screen

To open this screen, click **Basic Setting** > **xDSL Profiles Setup**.

Figure 56 Port Profile



Index	Name	Latency Mode	Down/ Up Stream Rate(kbps)	Select
1	DEFVAL	Interleave	100000/ 60000	●
2	DEFVAL_MAX	Interleave	100000/ 60000	○

Name		
Latency Mode	Interleave	
	Up Stream	Down Stream
Max Rate	128000 (64-128000)kbps	128000 (64-128000)kbps
Min Rate	64 (32-128000)kbps	64 (32-128000)kbps
Interleave Delay	20 (1-255) ms	20 (1-255) ms
Max SNR	31 (0-31) dB	31 (0-31) dB
Min SNR	0 (0-31) dB	0 (0-31) dB
Target SNR	6 (0-31) dB	6 (0-31) dB
Up Shift SNR	9 (0-31) dB	9 (0-31) dB
Down Shift SNR	3 (0-31) dB	3 (0-31) dB

The following table describes the labels in this screen.

Table 23 xDSL Port Profile

LABEL	DESCRIPTION
Index	This is the port profile index number.
Name	These are the names of individual profiles. The DEFVAL profile always exists and all of the DSL ports have it assigned to them by default. You can use up to 31 ASCII characters; spaces are not allowed.

Table 23 xDSL Port Profile (continued)

LABEL	DESCRIPTION
Latency Mode	This is the DSL latency mode (**Fast** or **Interleave**) for the ports that belong to this profile.
Down/Up Stream Rate (kbps)	These are the maximum downstream and upstream transfer rates for the ports that belong to this profile.
Select Modify	Select a profile's **Select** radio button and click **Modify** to edit the profile.
Select Delete	Select a profile's **Select** radio button and click **Delete** to remove the profile.
	The rest of the screen is for profile configuration.
Name	When editing a profile, this is the name of this profile. When adding a profile, type a name (up to 31 characters) for the profile.
Latency Mode	This field sets the DSL latency mode for the ports that belong to this profile. Select **Fast** mode to use no interleaving and have faster transmission (a "fast channel"). This would be suitable if you have a good line where little error correction is necessary. Select **Interleave** mode to use interleave delay when transmission error correction (Reed-Solomon) is necessary due to a less than ideal telephone line. See Section 16.3 on page 99 for more on interleave delay.
Up Stream	The following parameters relate to upstream transmissions.
Max Rate	Type a maximum upstream transfer rate (64 to 128000 Kbps) for this profile. Configure the maximum upstream transfer rate to be less than the maximum downstream transfer rate.
Min Rate	Type the minimum upstream transfer rate (32 to 128000 Kbps) for this port. Configure the minimum upstream transfer rate to be less than the maximum upstream transfer rate.
Interleave Delay	Configure this field if you set the **Latency Mode** field to **Interleave**. Type the number of milliseconds (1-255) of interleave delay to use for upstream transfers. It is recommended that you configure the same latency delay for both upstream and downstream.
Max SNR	Type the maximum upstream signal to noise margin (0-31 dB).
Min SNR	Type the minimum upstream signal to noise margin (0-31 dB). Configure the minimum upstream signal to noise margin to be less than or equal to the maximum upstream signal to noise margin.
Target SNR	Type the target upstream signal to noise margin (0-31 dB). Configure the target upstream signal to noise margin to be greater than or equal to the minimum upstream signal to noise margin and less than or equal to the maximum upstream signal to noise margin.
Up Shift SNR	The upstream up shift signal to noise margin (0-31 dB). When the channel's signal to noise margin goes above this number, the device can attempt to use a higher transfer rate. Configure the upstream up shift signal to noise margin to be greater than or equal to the target upstream signal to noise margin and less than or equal to the maximum upstream signal to noise margin.
Down Shift SNR	The upstream down shift signal to noise margin (0-31 dB). When the channel's signal to noise margin goes below this number, the device shifts to a lower transfer rate. Configure the upstream down shift signal to noise margin to be less than or equal to the target upstream signal to noise margin and greater than or equal to the minimum upstream signal to noise margin.
Down Stream	The following parameters relate to downstream transmissions.

Table 23 xDSL Port Profile (continued)

LABEL	DESCRIPTION
Max Rate	Type a maximum downstream transfer rate (64 to 128000 Kbps) bps for this port. Configure the maximum downstream transfer rate to be greater than the maximum upstream transfer rate.
Min Rate	Type the minimum downstream transfer rate (32 to 128000 Kbps) for this port. Configure the minimum downstream transfer rate to be less than the maximum downstream transfer rate.
Interleave Delay	Configure this field when you set the **Latency Mode** field to **interleave**. Type the number of milliseconds (1-255) of interleave delay to use for upstream transfers. It is recommended that you configure the same latency delay for both upstream and downstream.
Max SNR	Type the maximum downstream signal to noise margin (0-31 dB).
Min SNR	Type the minimum downstream signal to noise margin (0-31 dB). Configure the minimum downstream signal to noise margin to be less than or equal to the maximum downstream signal to noise margin.
Target SNR	Type the target downstream signal to noise margin (0-31 dB). Configure the target downstream signal to noise margin to be greater than or equal to the minimum downstream signal to noise margin and less than or equal to the maximum downstream signal to noise margin.
Up Shift SNR	The downstream up shift signal to noise margin (0-31 dB). When the channel's signal to noise margin goes above this number, the device can attempt to use a higher transfer rate. Configure the downstream up shift signal to noise margin to be greater than or equal to the target downstream signal to noise margin and less than or equal to the maximum downstream signal to noise margin.
Down Shift SNR	The downstream down shift signal to noise margin (0-31 dB). When the channel's signal to noise margin goes below this number, the device shifts to a lower transfer rate. Configure the downstream down shift signal to noise margin to be less than or equal to the target downstream signal to noise margin and greater than or equal to the minimum downstream signal to noise margin.
Add	Click **Add** to save your changes to the IP DSLAM's volatile memory. The IP DSLAM loses these changes if it is turned off or loses power, so use the **Config Save** link on the navigation panel to save your changes to the non-volatile memory when you are done configuring.
Cancel	Click **Cancel** to start configuring the screen again.

17.2 IPQoS Overview

Quality of Service (QoS) refers to both a network's ability to deliver data with minimum delay, and the networking methods used to control the use of bandwidth. Without QoS, all traffic data is equally likely to be dropped when the network is congested. This can cause a reduction in network performance and make the network inadequate for time-critical application such as video-on-demand.

A layer-2 classifier groups traffic according to the Ethernet type, VLAN group, MAC address and/or port number. A layer-3 classifier groups traffic according to the IP address and/or TCP/UDP protocol number.

Configure IPQoS on the IP DSLAM to group and prioritize application traffic in queues for downstream direction (toward CPE devices) and fine-tune network performance. Setting up IPQoS involves four parameters:

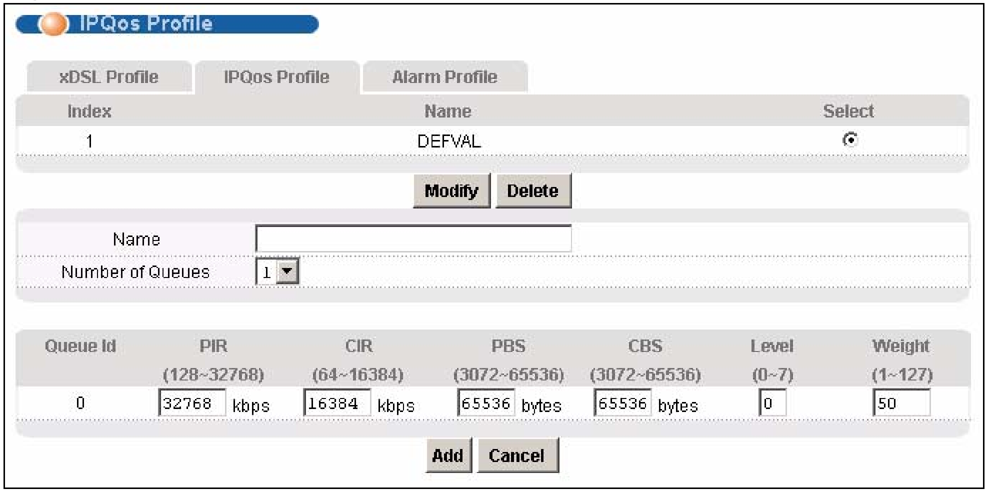
- PIR (Peak Information Rate): This is the maximum data rate allowed for the downstream traffic flowing through the IP DSLAM.
- CIR (Committed Information Rate): This is the guaranteed data rate for the downstream traffic flowing through the IP DSLAM.
- PBS (Peak Burst Size): This is the maximum burst size allowed for the downstream traffic flowing through the IP DSLAM when the burst data rate is between the predefined PIR and CIR.
- CBS (Committed Burst Size): This is the guaranteed burst size for the downstream traffic flowing through the IP DSLAM when the burst data rate is smaller than the predefined CIR.

17.2.1 IPQoS Profile Screen

Click **Basic Settings > xDSL Profile Setup > IPQos Profile** to open the following screen. Use this screen to configure the number of queues and QoS (Quality of Service) profile settings for each queue.

Use the second section of the screen to add or edit IPQoS profiles. The first section of the screen lists the configured IPQoS profiles.

Figure 57 IPQoS Profile



Index	Name	Select
1	DEFVAL	●

Name	
Number of Queues	1

Queue Id	PIR (128~32768)	CIR (64~16384)	PBS (3072~65536)	CBS (3072~65536)	Level (0~7)	Weight (1~127)
0	32768 kbps	16384 kbps	65536 bytes	65536 bytes	0	50

The following table describes the fields in this screen.

Table 24 IPQoS Profile

LABEL	DESCRIPTION
Index	This displays the index number of configured IPQoS profile(s).
Name	This displays the name of configured IPQoS profile(s).
Select	Select this next to an entry or entires that you want to edit or delete.
Modify	Click this to edit the selected profile.
Delete	Click this to remove the selected profile.
Name	Type a name to identify the IPQoS profile (you cannot change the name of the DEFVAL profile). You can use up to 31 English keyboard characters; spaces are not allowed.

Table 24 IPQoS Profile (continued)

LABEL	DESCRIPTION
Number of Queues	Select the number of queues used to classify traffic. You can select **1**, **2**, **4** or **8** queues in an IPQoS profile depending on the number of applications you want to classify. Note: It's highly recommended to use 8 queues for traffic classification.
Queue Id	This is the index number of queues listed in the following table according to what you selected in the **Number of Queues** field.
PIR	PIR is Peak Information Rate. Enter the maximum data rate (128~32768 kbps) allowed to flow through this device at peak hour. You must enter the number which is a multiple of 64. See Section 17.2 on page 119 for more information.
CIR	CIR is Committed Information Rate. Enter the maximum data rate (64~16384 kbps) guaranteed to flow through this device all the time. You must enter the number which is a multiple of 64. See Section 17.2 on page 119 for more information. Note: CIR < PIR <= two times of CIR in a queue. For example, CIR is 1024, you must enter the PIR in the same queue equal or less than 2048 (2 x 1024).
PBS	PBS is Peak Burst Size. Enter the maximum packet size (3072~65536 bytes) allowed to flow through this device at peak hour. You must enter the number which is a multiple of 256. See Section 17.2 on page 119 for more information.
CBS	CBS is Committed Burst Size. Enter the maximum packet size (3072~65536 bytes) guaranteed to flow through this device all the time. You must enter the number which is a multiple of 256. See Section 17.2 on page 119 for more information. Note: The CBS should be equal or less than PBS in a queue.
Level	Enter the priority level (0~7) for each queue. "0" is the lowest priority level and "7" is the highest.
Weight	Enter the queue weight (1~127) for each queue. The IP DSLAM services queues based on their priority level and queue weight rather than a fixed amount of bandwidth. Queues with larger weights get more service than queues with smaller weights. This queuing mechanism is highly efficient in that it divides any available bandwidth across the different traffic queues and returns to queues that have not yet emptied.
Add	Click **Add** to save what you configured in this screen and creates an IPQoS profile shown in the first section of the screen.
Cancel	Click **Cancel** to start configuring the screen again.

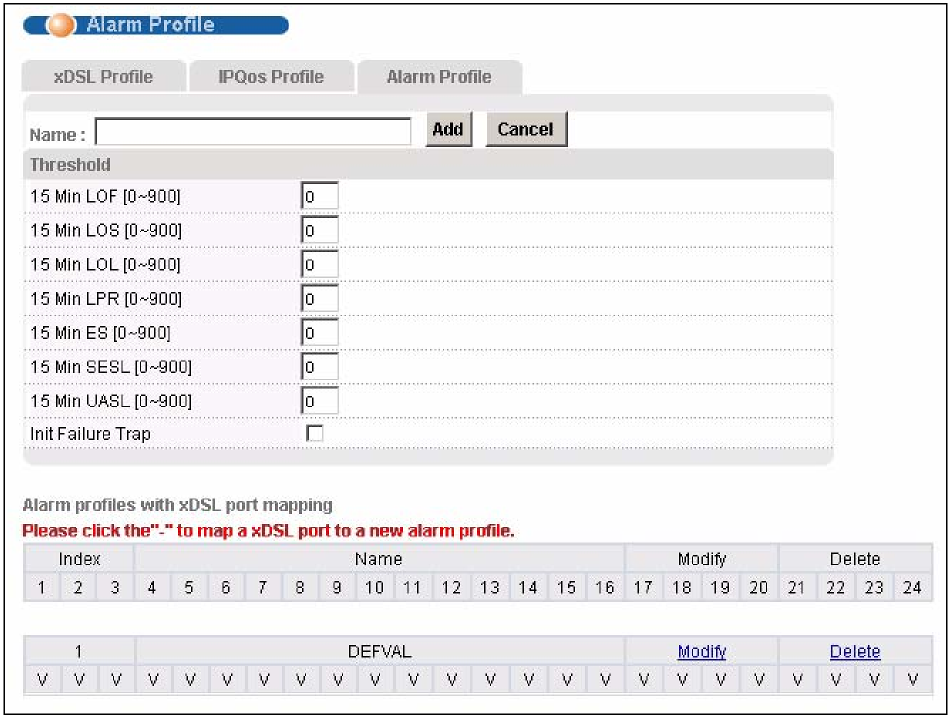
17.3 Alarm Profile Screen

Alarm profiles define VDSL port alarm thresholds. The IP DSLAM sends an alarm trap and generates a syslog entry when the thresholds of the alarm profile are exceeded.

To open this screen, click **Basic Setting** > **xDSL Profiles Setup** > **Alarm Profile**.

Use the top part of the screen (with the **Add** and **Cancel** buttons) to add or edit alarm profiles. The rest of the screen displays the configured alarm profiles.

Figure 58 Alarm Profile



Alarm Profile

xDSL Profile | IPQos Profile | Alarm Profile

Name : [ ] Add Cancel

Threshold

15 Min LOF [0~900]	0
15 Min LOS [0~900]	0
15 Min LOL [0~900]	0
15 Min LPR [0~900]	0
15 Min ES [0~900]	0
15 Min SESL [0~900]	0
15 Min UASL [0~900]	0
Init Failure Trap	□

Alarm profiles with xDSL port mapping

Please click the"-" to map a xDSL port to a new alarm profile.

Index			Name													Modify				Delete			
1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24
1			DEFVAL													Modify				Delete			
V	V	V	V	V	V	V	V	V	V	V	V	V	V	V	V	V	V	V	V	V	V	V	V

The following table describes the labels in this screen.

Table 25 Alarm Profile

LABEL	DESCRIPTION
Name	This field is read-only if you click **Modify** to edit a port profile. Type a name to identify the alarm profile (you cannot change the name of the DEFVAL profile). You can use up to 31 ASCII characters; spaces are not allowed.
Add	Click **Add** to save your changes to the IP DSLAM's volatile memory. The IP DSLAM loses these changes if it is turned off or loses power, so use the **Config Save** link on the navigation panel to save your changes to the non-volatile memory when you are done configuring.
Cancel	Click **Cancel** to start configuring the screen again.
Threshold	Specify limits for the individual performance counters. The IP DSLAM sends an alarm trap and generates a syslog entry when one of these thresholds is exceeded. A value of 0 disables the alarm threshold.
15 Min LOF	This field sets the limit for the number of Loss Of Frame seconds that are permitted to occur within 15 minutes.
15 Min LOS	This field sets the limit for the number of Loss Of Signal seconds that are permitted to occur within 15 minutes.
15 Min LOL	This field sets limit for the number of Loss Of Link seconds that are permitted to occur within 15 minutes.
15 Min LPR	This field sets the limit for the number of Loss of Power (on the XTUR) seconds that are permitted to occur within 15 minutes.
15 Min ES	This field sets the limit for the number of Errored Seconds that are permitted to occur within 15 minutes.
15 Min SESL	This field sets the limit for the number of Severely Errored seconds that are permitted to occur within 15 minutes.
15 Min UASL	This field sets the limit for the number of UnAvailable seconds that are permitted to occur within 15 minutes.

Table 25 Alarm Profile (continued)

LABEL	DESCRIPTION
Init Failure Trap	Select this to trigger an alarm for an initialization failure trap.
Alarm profiles with xDSL port mapping	After you add an alarm profile, you can click a port number’s “**-**“ symbol to map the xDSL port to that alarm profile. The port’s “**V**” symbol in the alarm profile where it was previously mapped changes to “**-**“.
Modify	Click **Modify** to edit a profile.
Delete	Click **Delete** to remove a profile.

18

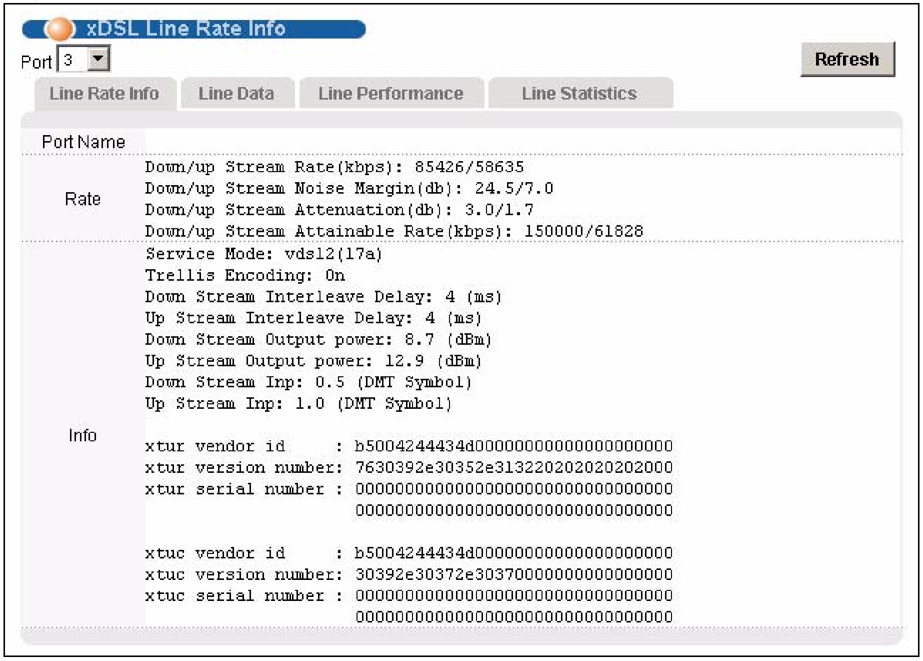
xDSL Line Data

18.1 xDSL Line Rate Info Screen

This screen displays a VDSL port’s line operating values. Information obtained prior to training to steady state transition will not be valid or will be old information.

To open this screen, click **Basic Setting** > **xDSL Line Data**.

Figure 59 xDSL Line Rate Info



Port Name

Rate

```
Down/up Stream Rate(kbps): 85426/58635
Down/up Stream Noise Margin(db): 24.5/7.0
Down/up Stream Attenuation(db): 3.0/1.7
Down/up Stream Attainable Rate(kbps): 150000/61828
```

Info

```
Service Mode: vdsl2(17a)
Trellis Encoding: On
Down Stream Interleave Delay: 4 (ms)
Up Stream Interleave Delay: 4 (ms)
Down Stream Output power: 8.7 (dBm)
Up Stream Output power: 12.9 (dBm)
Down Stream Inp: 0.5 (DMT Symbol)
Up Stream Inp: 1.0 (DMT Symbol)

xtur vendor id     : b5004244434d00000000000000000000
xtur version number: 7630392e30352e313220202020202000
xtur serial number : 00000000000000000000000000000000
                     00000000000000000000000000000000

xtuc vendor id     : b5004244434d00000000000000000000
xtuc version number: 30392e30372e30370000000000000000
xtuc serial number : 00000000000000000000000000000000
                     00000000000000000000000000000000
```

The following table describes the labels in this screen.

Table 26 xDSL Line Rate Info

LABEL	DESCRIPTION
Port	Use this drop-down list box to select a port for which you wish to view information.
Refresh	Click **Refresh** to display updated information.
Port Name	This section displays the name of the configured DSL port.
Rate	The rate fields display the transmission rates. “Link Down” indicates that the DSL port is not connected to a subscriber.
Down/up Stream Rate	These are the rates (in Kbps) at which the port has been sending and receiving data.

Table 26 xDSL Line Rate Info (continued)

LABEL	DESCRIPTION
Down/up Stream Noise Margin	These are the DSL line’s downstream and upstream noise margins. Measured in decibels (dB).
Down/up Stream Attenuation	These are the reductions in amplitude of the downstream and upstream DSL signals. Measured in decibels (dB).
Down/up Stream Attainable Rate	These are the highest theoretically possible transfer rates (in Kbps) at which the port could send and receive data.
Info	
Service Mode	This field displays the VDSL or ADSL standard that the port is currently using.
Trellis Encoding	This field displays whether Trellis encoding is turned on or off. Trellis encoding helps to reduce the noise in xDSL transmissions. Trellis may reduce throughput but it makes the connection more stable.[A]
Down Stream Interleave Delay	This field displays the number of milliseconds of interleave delay for downstream transmissions.
Up Stream Interleave Delay	This field displays the number of milliseconds of interleave delay for upstream transmissions.
Down Stream Output Power	This field displays the amount of power that this port is using to transmit to the subscriber’s xDSL modem. The total output power of the transceiver varies with the length and line quality. The farther away the subscriber’s xDSL modem or router is or the more interference there is on the line, the more power is needed.
Up Stream Output Power	This field displays the amount of power that the subscriber’s xDSL modem or router is using to transmit to this port. The total output power of the transceiver varies with the length and line quality. The farther away the subscriber’s xDSL modem or router is or the more interference there is on the line, the more power is needed.
Down Stream Inp	This field displays the number of impulse noise protection DMT symbols in downstream transmissions.
Up Stream Inp	This field displays the number of impulse noise protection DMT symbols in upstream transmissions.
Info xtur Info xtuc	The **Info xtur** fields show data acquired from the xTUR (xDSL Termination Unit – Remote), in this case the subscriber’s xDSL modem or router, during negotiation/provisioning message interchanges. This information can help in identifying the subscriber’s xDSL modem or router. The **Info xtuc** fields show data acquired from the xTUC (xDSL Termination Unit – Central), in this case IP DSLAM, during negotiation/provisioning message interchanges.

A. At the time of writing, the IP DSLAM always uses Trellis coding.

18.2 xDSL Line Data Screen

This screen displays an xDSL port’s line bit allocation.

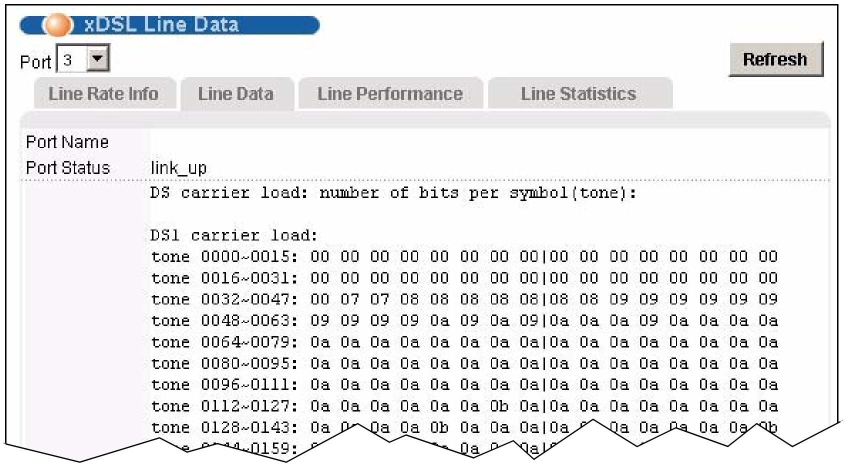
Discrete Multi-Tone (DMT) modulation divides up a line’s bandwidth into tones. This screen displays the number of bits transmitted for each tone. This can be used to determine the quality of the connection, whether a given sub-carrier loop has sufficient margins to support xDSL transmission rates, and possibly to determine whether certain specific types of interference or line attenuation exist.

The better (or shorter) the line, the higher the number of bits transmitted for a DMT tone. The maximum number of bits that can be transmitted per DMT tone is 15.

The bit allocation contents are only valid when the link is up.

To open this screen, click **Basic Setting** > **xDSL Line Data** > **Line Data**.

Figure 60 xDSL Line Data



Port Name

Port Status link_up

```
DS carrier load: number of bits per symbol(tone):

DS1 carrier load:
tone 0000~0015: 00 00 00 00 00 00 00 00|00 00 00 00 00 00 00 00
tone 0016~0031: 00 00 00 00 00 00 00 00|00 00 00 00 00 00 00 00
tone 0032~0047: 00 07 07 08 08 08 08 08|08 08 09 09 09 09 09 09
tone 0048~0063: 09 09 09 09 0a 09 0a 09|0a 0a 0a 09 0a 0a 0a 0a
tone 0064~0079: 0a 0a 0a 0a 0a 0a 0a 0a|0a 0a 0a 0a 0a 0a 0a 0a
tone 0080~0095: 0a 0a 0a 0a 0a 0a 0a 0a|0a 0a 0a 0a 0a 0a 0a 0a
tone 0096~0111: 0a 0a 0a 0a 0a 0a 0a 0a|0a 0a 0a 0a 0a 0a 0a 0a
tone 0112~0127: 0a 0a 0a 0a 0a 0a 0b 0a|0a 0a 0a 0a 0a 0a 0a 0a
tone 0128~0143: 0a    0a 0a 0b 0a 0a 0a|0a    0a 0a    0a 0a 0b
```

The following table describes the labels in this screen.

Table 27 xDSL Line Data

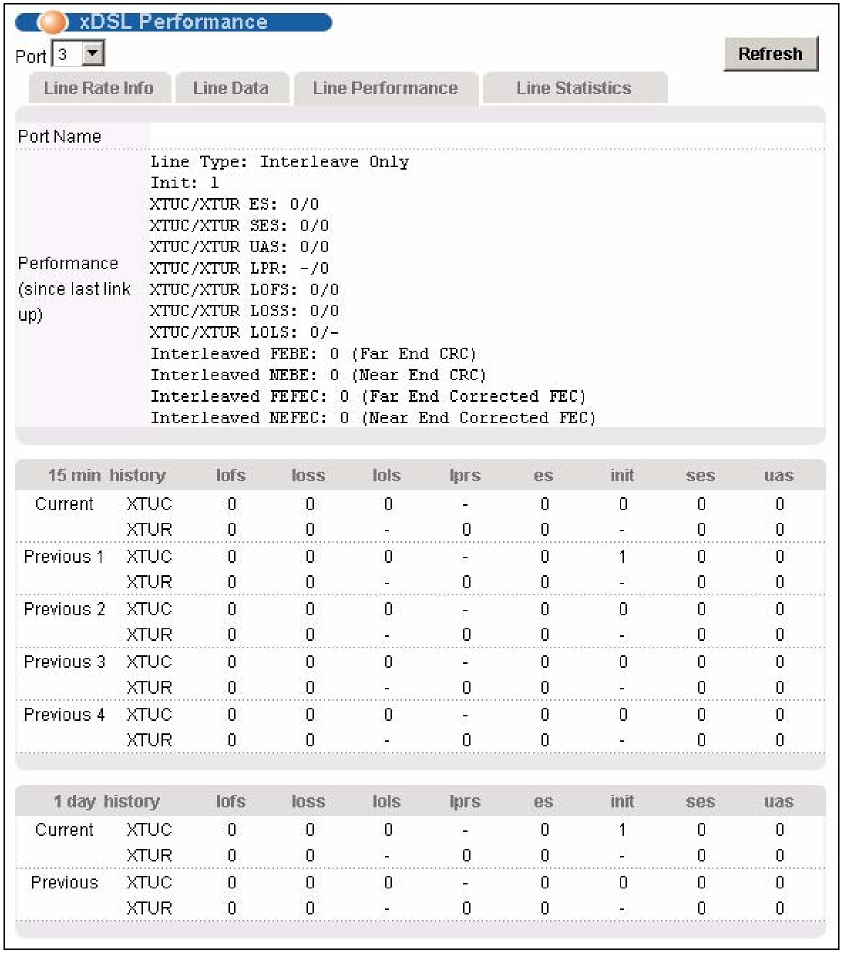
LABEL	DESCRIPTION
Port	Use this drop-down list box to select a port for which you wish to view information.
Refresh	Click **Refresh** to display updated information.
Port Name	This section displays the name of the DSL port.
Port Status	This field displays the current status (**link_up** or **link_down**) of the DSL port.
Bit Allocation	**DSX carrier load** displays the number of bits transmitted per DMT tone for the downstream channel (from the IP DSLAM to the subscriber's DSL modem or router). **USX carrier load** displays the number of bits received per DMT tone for the upstream channel (from the subscriber's DSL modem or router to the IP DSLAM).

18.3 xDSL Performance Screen

These counters display line performance data that has been accumulated since the system started. The definitions of near end/far end are always relative to the xTU-C (xDSL Termination Unit-Central Office). xTU-C refers to downstream traffic from the IP DSLAM. xTU-R (xDSL Termination Unit-Remote) refers to upstream traffic from the subscriber.

To open this screen, click **Basic Setting** > **xDSL Line Data** > **Line Performance**.

Figure 61 xDSL Performance



Port 3

Port Name

Performance (since last link up)

```
Line Type: Interleave Only
Init: 1
XTUC/XTUR ES: 0/0
XTUC/XTUR SES: 0/0
XTUC/XTUR UAS: 0/0
XTUC/XTUR LPR: -/0
XTUC/XTUR LOFS: 0/0
XTUC/XTUR LOSS: 0/0
XTUC/XTUR LOLS: 0/-
Interleaved FEBE: 0 (Far End CRC)
Interleaved NEBE: 0 (Near End CRC)
Interleaved FEFEC: 0 (Far End Corrected FEC)
Interleaved NEFEC: 0 (Near End Corrected FEC)
```

15 min history		lofs	loss	lols	lprs	es	init	ses	uas
Current	XTUC	0	0	0	-	0	0	0	0
	XTUR	0	0	-	0	0	-	0	0
Previous 1	XTUC	0	0	0	-	0	1	0	0
	XTUR	0	0	-	0	0	-	0	0
Previous 2	XTUC	0	0	0	-	0	0	0	0
	XTUR	0	0	-	0	0	-	0	0
Previous 3	XTUC	0	0	0	-	0	0	0	0
	XTUR	0	0	-	0	0	-	0	0
Previous 4	XTUC	0	0	0	-	0	0	0	0
	XTUR	0	0	-	0	0	-	0	0

1 day history		lofs	loss	lols	lprs	es	init	ses	uas
Current	XTUC	0	0	0	-	0	1	0	0
	XTUR	0	0	-	0	0	-	0	0
Previous	XTUC	0	0	0	-	0	0	0	0
	XTUR	0	0	-	0	0	-	0	0

The following table describes the labels in this screen.

Table 28 xDSL Performance

LABEL	DESCRIPTION
Port	Use this drop-down list box to select a port for which you wish to view information.
Refresh	Click **Refresh** to display updated information.
Port Name	This section displays the name of the DSL port.
Performance (since last link up)	
Line Type	“Fast” stands for non-interleaved (fast mode) and “Interleaved” stands for interleaved mode.
Init	This field displays the number of link-ups and link-downs.
XTUC/XTUR ES	The Number of Errored Seconds transmitted (downstream) or received (upstream) on this DSL port.
XTUC/XTUR SES	The Number of Severely Errored Seconds transmitted (downstream) or received (upstream) on this DSL port. Severely errored seconds contained 30% or more errored blocks or at least one defect. This is a subset of the **Down/Up Stream ES**.
XTUC/XTUR UAS	The downstream or upstream number of UnAvailable Seconds.

Table 28 xDSL Performance (continued)

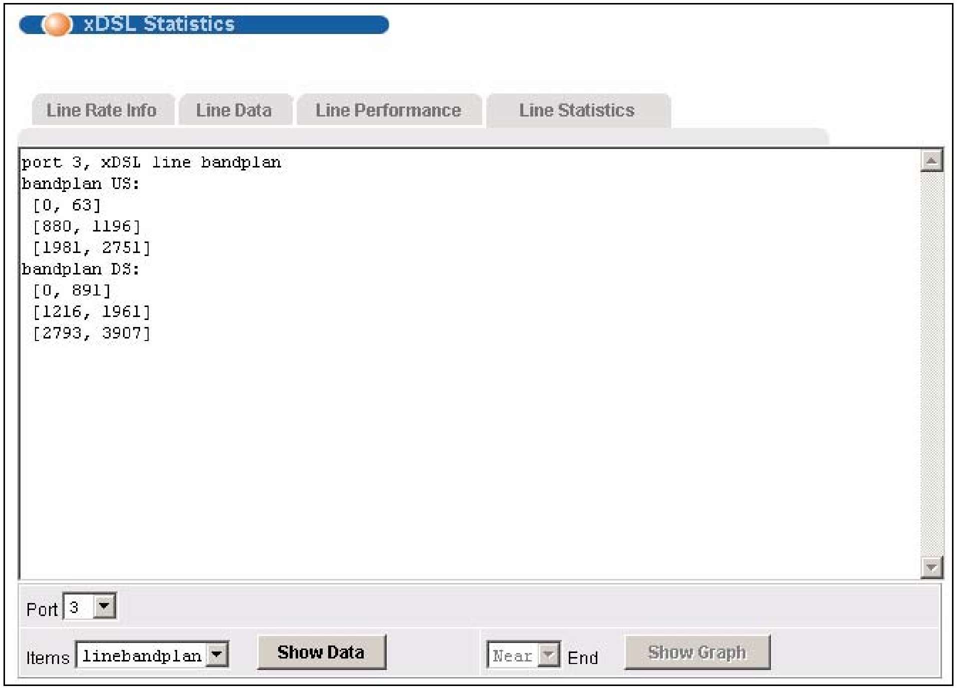
LABEL	DESCRIPTION
XTUC/XTUR LPR	This is the number of times the DSL line’s upstream connection has experienced a Loss of power.
XTUC/XTUR LOFS	These are the DSL line’s downstream and upstream numbers of Loss of frame Seconds.
XTUC/XTUR LOSS	These are the DSL line’s downstream and upstream numbers of Loss of signal Seconds.
XTUC/XTUR LOLS	This is the DSL line’s downstream number of Loss of link Seconds.
Interleaved FEBE	In interleaved mode, the number of Far End Block Errors (Far End Cyclic Redundancy Checks).
Interleaved NEBE	In interleaved mode, the number of Near End Block Errors (Near End Cyclic Redundancy Checks).
Interleaved FEFEC	In interleaved mode, the Far End number of DSL frames repaired by Forward Error Correction.
Interleaved NEFEC	In interleaved mode, the Near End number of DSL frames repaired by Forward Error Correction.
15 min, 1day history	These sections of the screen display line performance statistics for the current and previous 15-minute periods, as well as for the current and previous 24 hours.
lofs	The number of Loss Of Frame Seconds that have occurred within the period.
loss	The number of Loss Of Signal Seconds that have occurred within the period.
lols	The number of Loss Of Link Seconds that have occurred within the period.
lprs	The number of Loss of Power Seconds that have occurred within the period.
es	The number of Errored Seconds that have occurred within the period.
init	The number of successful initializations that have occurred within the period.
ses	The number of Severely Errored Seconds that have occurred within the period.
uas	The number of UnAvailable Seconds that have occurred within the period.

18.4 xDSL Statistics Screen

Use this screen to display DSL line statistics for details about the line quality and channel conditions.

To open this screen, click **Basic Setting** > **xDSL Line Data** > **Line Statistics**.

Figure 62 xDSL Statistics



```
port 3, xDSL line bandplan
bandplan US:
 [0, 63]
 [880, 1196]
 [1981, 2751]
bandplan DS:
 [0, 891]
 [1216, 1961]
 [2793, 3907]
```

Port 3

Items linebandplan

Near End

The following table describes the labels in this screen.

Table 29 xDSL Statistics

LABEL	DESCRIPTION
Port	Select a port number on which you want to display related line statistics.
Items, Show Data	Select one of the following items and click **Show Data** to display the statistics result in this screen. • Select **linebandplan** to see the line's band plan arrangement for upstream and downstream transmissions. • Select **linegain** to see the line's gain values per tone measured for upstream and downstream transmissions. • Select **linehlog** (Channel Transfer Function per sub-carrier) to see the line's capability against attenuation. The format provides magnitude values in a logarithmic scale. • Select **lineqln** (Quiet Line Noise per sub-carrier) to analyze crosstalk on the line. • Select **linesnr** (Signal-to-Noise-Ratio per sub-carrier) to see the line's signal strength level by calculating the ratio between the received signal power and the received noise power for each sub-carrier. • Select **linetssi** to display the VDSL line TSSI parameters. • Select **resultmask** to see the line's PSD mask adjustment result according to your VDSL settings on the port.
Near/Far End, Show Graph	When you select **linehlog**, **lineqln** or **linesnr** in the **Items** field, you can select this and click **Show Graph** to additionally show DSL Sub-Carrier statistics in a prompted graph. • Select **Near End** to see the upstream line statistics of the selected item. • Select **Far End** to see the downstream line statistics of the selected item.

PART III Advanced Application

19

VLAN

This chapter shows you how to configure IEEE 802.1Q tagged VLANs.

19.1 Introduction to VLANs

A VLAN (Virtual Local Area Network) allows a physical network to be partitioned into multiple logical networks. Devices on a logical network belong to one group. A device can belong to more than one group. With VLAN, a device cannot directly talk to or hear from devices that are not in the same group(s); the traffic must first go through a router.

In MTU (Multi-Tenant Unit) applications, VLAN is vital in providing isolation and security among the subscribers. When properly configured, VLAN prevents one subscriber from accessing the network resources of another on the same LAN, thus a user will not see the printers and hard disks of another user in the same building.

VLAN also increases network performance by limiting broadcasts to a smaller and more manageable logical broadcast domain. In traditional switched environments, all broadcast packets go to each and every individual port. With VLAN, all broadcasts are confined to a specific broadcast domain.

Note that a VLAN is unidirectional, it only governs outgoing traffic.

19.2 Introduction to IEEE 802.1Q Tagged VLAN

Tagged VLAN uses an explicit tag (VLAN ID) in the MAC header to identify the VLAN membership of a frame across bridges - they are not confined to the device on which they were created. The VLANs can be created statically by hand. The VLAN ID associates a frame with a specific VLAN and provides the information that devices need to process the frame across the network. A tagged frame is four bytes longer than an untagged frame and contains two bytes of TPID (Tag Protocol Identifier, residing within the type/length field of the Ethernet frame) and two bytes of TCI (Tag Control Information, starts after the source address field of the Ethernet frame).

The CFI (Canonical Format Indicator) is a single-bit flag, always set to zero for Ethernet switches. If a frame received at an Ethernet port has a CFI set to 1, then that frame should not be forwarded as it is to an untagged port. The remaining twelve bits define the VLAN ID, giving a possible maximum number of 4,096 (2^{12}) VLANs. Note that user priority and VLAN ID are independent of each other. A frame with VID (VLAN Identifier) of null (0) is called a priority frame, meaning that only the priority level is significant and the default VID of the ingress port is given as the VID of the frame. Of the 4096 possible VIDs, a VID of 0 is used to identify priority frames and value 4095 (FFF) is reserved, so the maximum possible VLAN configurations are 4,094. See Chapter 54 on page 283 for the maximum number of VLANs the IP DSLAM can support.

TPID 2 Bytes	User Priority 3 Bits	CFI 1 Bit	VLAN ID 12 bits

The IP DSLAM handles up to 4094 VLANs (VIDs 1-4094). The device accepts incoming frames with VIDs 1-4094.

19.2.1 Forwarding Tagged and Untagged Frames

Each port on the device is capable of passing tagged or untagged frames. To forward a frame from an 802.1Q VLAN-aware switch to an 802.1Q VLAN-unaware switch, the IP DSLAM first decides where to forward the frame and then strips off the VLAN tag. To forward a frame from an 802.1Q VLAN-unaware switch to an 802.1Q VLAN-aware switch, the IP DSLAM first decides where to forward the frame, and then inserts a VLAN tag reflecting the ingress port's default VID. The default PVID is VLAN 1 for all ports, but this can be changed.

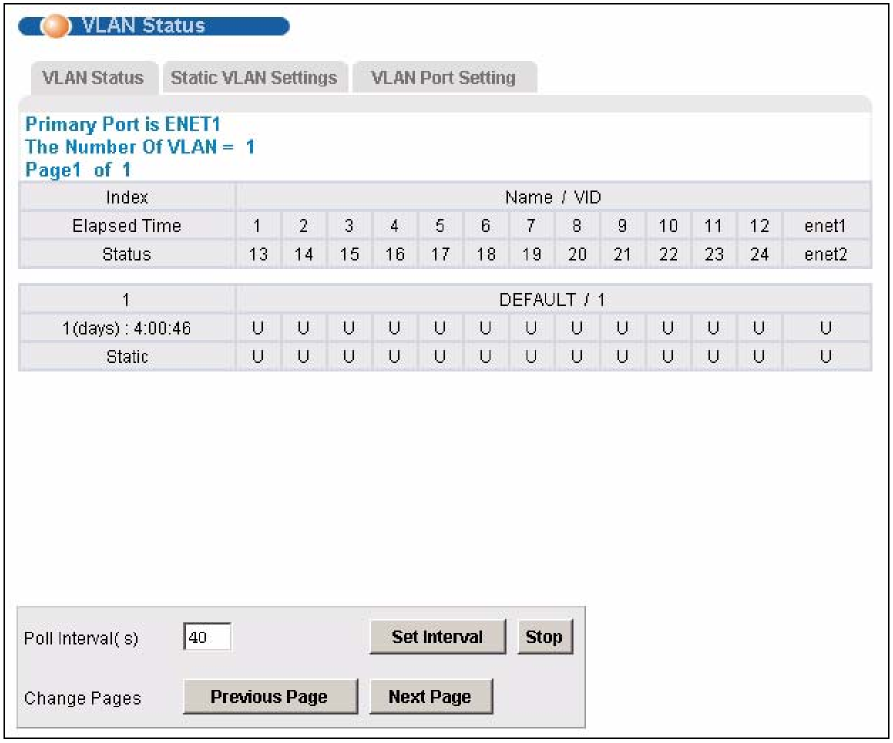
The egress (outgoing) port(s) of a frame is determined on the combination of the destination MAC address and the VID of the frame. For a unicast frame, the egress port (based on the destination MAC address) must be a member of the VID, also; otherwise, the frame is blocked. For a broadcast frame, it is duplicated only on ports (except the ingress port itself) that are members of the VID, thus confining the broadcast to a specific domain.

Whether to tag an outgoing frame depends on the setting of the egress port on a per-VLAN, per-port basis (recall that a port can belong to multiple VLANs). If the tagging on the egress port is enabled for the VID of a frame, then the frame is transmitted as a tagged frame; otherwise, it is transmitted as an untagged frame.

19.3 VLAN Status Screen

To open this screen, click **Advanced Application** > **VLAN**.

Figure 63 VLAN Status



Primary Port is ENET1
The Number Of VLAN = 1
Page1 of 1

Index	Name / VID												
Elapsed Time	1	2	3	4	5	6	7	8	9	10	11	12	enet1
Status	13	14	15	16	17	18	19	20	21	22	23	24	enet2

1	DEFAULT / 1												
1(days) : 4:00:46	U	U	U	U	U	U	U	U	U	U	U	U	U
Static	U	U	U	U	U	U	U	U	U	U	U	U	U

Poll Interval(s) 40

Change Pages

The following table describes the labels in this screen.

Table 30 VLAN Status

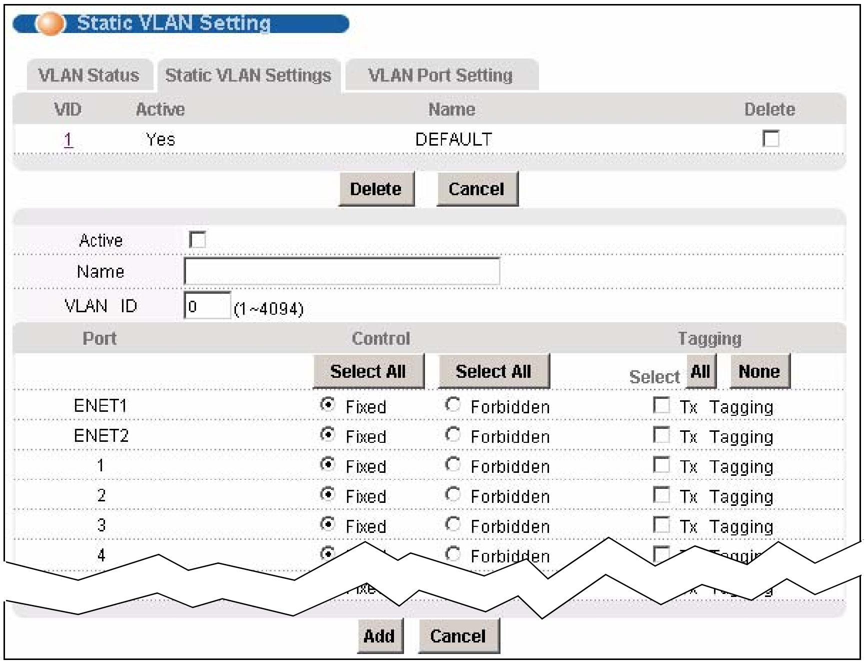
LABEL	DESCRIPTION
The Number Of VLAN	This is the number of VLANs configured on the IP DSLAM.
Page X of Y	This identifies which page of VLAN status information is displayed and how many total pages of VLAN status information there are.
	The first table displays the names of the fields. The subsequent tables show the settings of the VLANs.
Index	This is the VLAN index number.
Name / VID	The name identifies an individual VLAN. The vid is the PVID, the Port VLAN ID assigned to untagged frames or priority-tagged frames received on this port.
1~24, enet1, enet2	These columns display the VLAN’s settings for each port. A tagged port is marked as **T**, an untagged port is marked as **U** and ports not participating in a VLAN are marked as “**–**“.
Elapsed Time	This field shows how long it has been since a normal VLAN was registered or a static VLAN was set up.
Status	This field shows that this VLAN was added to the IP DSLAM statically, that is, added as a permanent entry.
Poll Interval(s) Set Interval	The text box displays how often (in seconds) this screen refreshes. You may change the refresh interval by typing a new number in the text box and then clicking **Set Interval**.
Stop	Click **Stop** to halt polling statistics.
Previous Page Next Page	Click one of these buttons to show the preceding/following screen if the information cannot be displayed in one screen.

19.4 Static VLAN Setting Screen

You can assign a port to be a member of a VLAN group or prohibit a port from joining a VLAN group in this screen. This is an IEEE 802.1Q VLAN.

To open this screen, click **Advanced Application** > **VLAN** > **Static VLAN Setting**.

Figure 64 Static VLAN Setting



VID	Active	Name	Delete
1	Yes	DEFAULT	□

Active □

Name

VLAN ID 0 (1~4094)

Port	Control		Tagging
ENET1	● Fixed	○ Forbidden	□ Tx Tagging
ENET2	● Fixed	○ Forbidden	□ Tx Tagging
1	● Fixed	○ Forbidden	□ Tx Tagging
2	● Fixed	○ Forbidden	□ Tx Tagging
3	● Fixed	○ Forbidden	□ Tx Tagging
4	●	○ Forbidden	□

The following table describes the labels in this screen.

Table 31 Static VLAN Setting

LABEL	DESCRIPTION
VID	This field displays the ID number of the VLAN group. Click the number to edit the VLAN settings.
Active	This field indicates whether the VLAN settings are enabled (**Yes**) or disabled (**No**).
Name	This field displays the descriptive name for this VLAN group.
Delete	Select the check boxes of the rule(s) that you want to remove in the **Delete** column and then click the **Delete** button. You cannot delete a VLAN if any PVIDs are set to use the VLAN or the VLAN is the CPU (management) VLAN.
Cancel	Click **Cancel** to clear the **Delete** check boxes.
Active	Select this check box to enable the VLAN. You cannot disable a VLAN if any PVIDs are set to use the VLAN or the VLAN is the CPU (management) VLAN.
Name	Enter a descriptive name for this VLAN group for identification purposes. Spaces are not allowed.
VLAN ID	Enter the VLAN ID for this static VLAN entry; the valid range is between 1 and 4094.
Port	The port numbers identify the IP DSLAM's ports.

Table 31 Static VLAN Setting (continued)

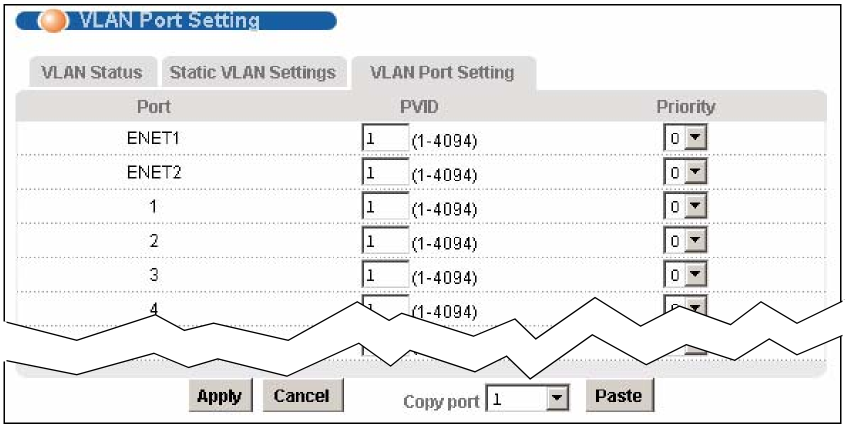
LABEL	DESCRIPTION
Control	Select **Fixed** for the port to be a permanent member of this VLAN group. Use the **Select All** button to include every port. Select **Forbidden** if you want to prohibit the port from joining this VLAN group. Use the **Select All** button to include every port.
Tagging	Select **TX Tagging** if you want the port to tag all outgoing frames transmitted with this VLAN ID. Use the **All** button to include every port. Use the **None** button to clear all of the ports check boxes.
Add	Click **Add** to save your settings. The VLAN then displays in the summary table at the top of the screen. Clicking **Add** saves your changes to the IP DSLAM’s volatile memory. The IP DSLAM loses these changes if it is turned off or loses power, so use the **Config Save** link on the navigation panel to save your changes to the non-volatile memory when you are done configuring.
Cancel	Click **Cancel** to begin configuring the fields afresh.

19.5 VLAN Port Setting Screen

Use this screen to specify port VLAN IDs and to set whether or not Ethernet ports propagate VLAN information to other devices.

To open this screen, click **Advanced Application** > **VLAN** > **VLAN Port Setting**.

Figure 65 VLAN Port Setting



Port	PVID	Priority
ENET1	1 (1-4094)	0
ENET2	1 (1-4094)	0
1	1 (1-4094)	0
2	1 (1-4094)	0
3	1 (1-4094)	0
4	(1-4094)	

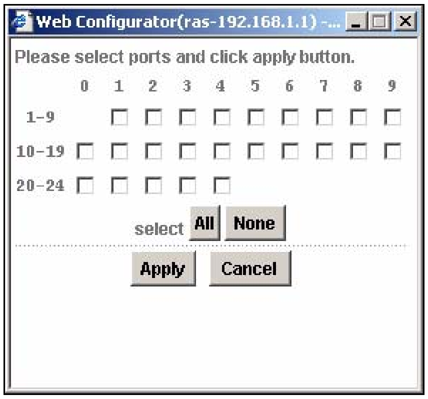
Copy port 1

The following table describes the labels in this screen.

Table 32 VLAN Port Setting

LABEL	DESCRIPTION
Port	The port numbers identify the IP DSLAM’s ports.
PVID	Type the Port VLAN ID (PVID) from 1 to 4094. The IP DSLAM assigns the PVID to untagged frames or priority frames (0 VID) received on this port.
Priority	Select an IEEE 802.1p priority to assign to untagged frames or priority frames (0 VID) received on this port.

Table 32 VLAN Port Setting (continued)

LABEL	DESCRIPTION
Apply	Click **Apply** to save your changes to the IP DSLAM's volatile memory. The IP DSLAM loses these changes if it is turned off or loses power, so use the **Config Save** link on the navigation panel to save your changes to the non-volatile memory when you are done configuring.
Cancel	Click **Cancel** to begin configuring this screen afresh.
Copy port Paste	Do the following to copy settings from one port to another port or ports. 1. Select the number of the port from which you want to copy settings. 2. Click **Paste** and the following screen appears. 3. Select to which ports you want to copy the settings. Use **All** to select every port. Use **None** to clear all of the check boxes. 4. Click **Apply** to paste the settings. **Figure 66** Select Ports  Please select ports and click apply button. Web Configurator(ras-192.168.1.1) -... 0 1 2 3 4 5 6 7 8 9 1-9 □ □ □ □ □ □ □ □ □ 10-19 □ □ □ □ □ □ □ □ □ □ 20-24 □ □ □ □ □ select All None Apply Cancel

20

Protocol VLAN

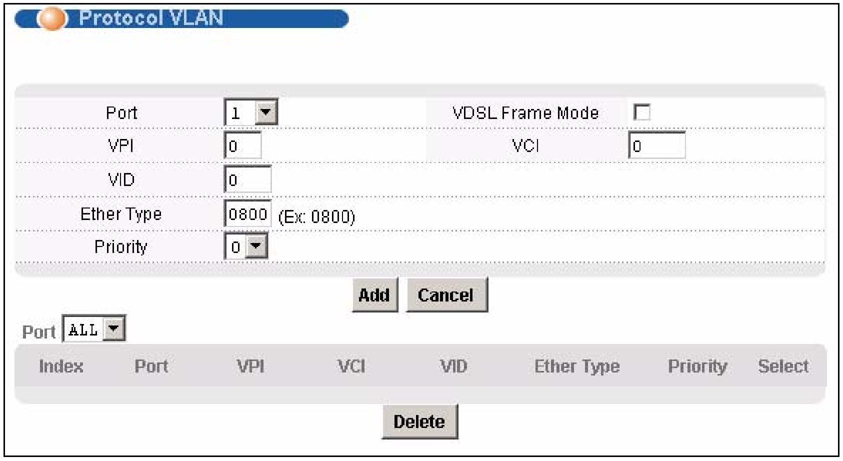
20.1 Protocol-based VLAN

With protocol-based VLAN (PVLAN), “802.1Q untagged” packet will be tagged a VLAN ID based on its protocol. Enable this feature on a port when you want to convert the VLAN untagged packets (sent from the connected CPE device) to VLAN-tagged packets which are then allowed to flow into a VLAN-tagged switch network for specified traffic. You can set different VLANs for different application traffic on a port. For example, you can define 0806 (ARP) and 0800 (IP) on a port. Then untagged ARP and IP traffic will be tagged with the specified VLAN IDs. The other untagged packets will be tagged with each port’s PVID VLAN depending on through which port the packets flow.

20.1.1 The Protocol VLAN Screen

Use this screen to add or remove a VLAN tag from specific traffic flowing through a specified port. To open this screen, click **Advanced Application** > **Protocol VLAN**.

Figure 67 Protocol VLAN



Protocol VLAN

Port	1	VDSL Frame Mode	□
VPI	0	VCI	0
VID	0		
Ether Type	0800 (Ex: 0800)		
Priority	0		

Index	Port	VPI	VCI	VID	Ether Type	Priority	Select

The following table describes the fields in this screen.

Table 33 Protocol VLAN

LABEL	DESCRIPTION
Port	Select which port through which you want apply this protocol VLAN tag to the traffic flowing.
VDSL Frame Mode	Select this for a VDSL port or clear this for an ADSL port.

Table 33 Protocol VLAN

LABEL	DESCRIPTION
VPI	Type the Virtual Path Identifier for the ADSL PVC. This field is available if you clear the **VDSL Frame Mode** field.
VCI	Type the Virtual Circuit Identifier for the ADSL PVC. This field is available if you clear the **VDSL Frame Mode** field. Note: The PVC must be a super channel (see Section 16.11 on page 113) and the associated VLAN must be created first.
VID	Specify a VLAN ID (1~4094).
Ether Type	Enter 4 digits in hexadecimal for Ethernet type which specify a protocol traffic. For example, 0806 is the Ethernet type, 0x0806, for ARP (Address Resolution Protocol) traffic.
Priority	Enter the priority level for the protocol VLAN. "0" is the lowest priority level and "7" is the highest.
Add	Click **Add** to save the changes in this screen to the system's volatile memory. The system loses these changes if it is turned off or loses power, so use the **Config Save** on the navigation panel to save your changes to the non-volatile memory when you are done configuring.
Cancel	Click **Cancel** to begin configuring the screen again.
The table in the bottom half of the screen lists the VLANs that specific untagged traffic belongs to.	
Index	This is the index number of records in the table.
Port	This field displays the port number for the specified VC.
VPI	This field displays the Virtual Path Identifier for the specified ADSL PVC.
VCI	This field displays the Virtual Circuit Identifier for the specified ADSL PVC.
VID	This field displays a VLAN (VLAN ID) to which a specific traffic will be assigned.
Ether Type	This field displays Ethernet types to specify a certain protocol traffic.
Priority	This field displays the priority for the protocol VLAN.
Select Delete	Select the radio button of a VLAN membership entry and then use the **Delete** button to remove an entry.

21

IGMP

This chapter describes the **IGMP** screens.

21.1 IGMP

Traditionally, IP packets are transmitted in one of either two ways - Unicast (1 sender to 1 recipient) or Broadcast (1 sender to everybody on the network). Multicast delivers IP packets to just a group of hosts on the network.

IGMP (Internet Group Multicast Protocol) is a network-layer protocol used to establish membership in a multicast group - it is not used to carry user data. See RFC 1112, RFC 2236, and RFC 3376 for information on IGMP versions 1, 2, and 3, respectively.

21.2 IP Multicast Addresses

In IPv4, a multicast address allows a device to send packets to a specific group of hosts (multicast group) in a different sub-network. A multicast IP address represents a traffic receiving group, not individual receiving devices. IP addresses in the Class D range (224.0.0.0 to 239.255.255.255) are used for IP multicasting. Certain IP multicast numbers are reserved by IANA for special purposes (see the IANA web site for more information).

21.2.1 IGMP Snooping

A layer-2 switch can passively snoop on IGMP Query, Report and Leave (IGMP version 2 or 3) packets transferred between IP multicast routers/switches and IP multicast hosts to learn the IP multicast group membership. It checks IGMP packets passing through it, picks out the group registration information, and configures multicasting accordingly. IGMP snooping allows the IP DSLAM to learn multicast groups without you having to manually configure them.

The IP DSLAM forwards multicast traffic destined for multicast groups (that it has learned from IGMP snooping or that you have manually configured) to ports that are members of that group. The IP DSLAM discards multicast traffic destined for multicast groups that it does not know. IGMP snooping generates no additional network traffic, allowing you to significantly reduce multicast traffic passing through your device.

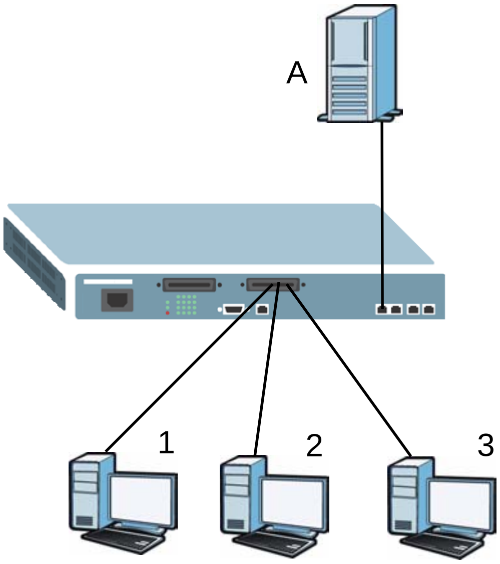
21.2.2 IGMP Proxy

To allow better network performance, you can use IGMP proxy instead of a multicast routing protocol in a simple tree network topology.

In IGMP proxy, an upstream interface is the port that is closer to the source (or the root of the multicast tree) and is able to receive multicast traffic. There should only be one upstream interface (also known as the query port) for one query VLAN on the IP DSLAM. A downstream interface is a port that connects to a host (such as a computer).

The following figure shows a network example where **A** is the multicast source while computers **1**, **2** and **3** are the receivers. In the figure **A** is connected to the upstream interface and **1**, **2** and **3** are connected to the downstream interface.

Figure 68 IGMP Proxy Network Example



The IP DSLAM will not respond to IGMP join and leave messages on the upstream interface. The IP DSLAM only responds to IGMP query messages on the upstream interface. The IP DSLAM sends IGMP query messages to the hosts that are members of the query VLAN.

The IP DSLAM only sends an IGMP leave messages via the upstream interface when the last host leaves a multicast group.

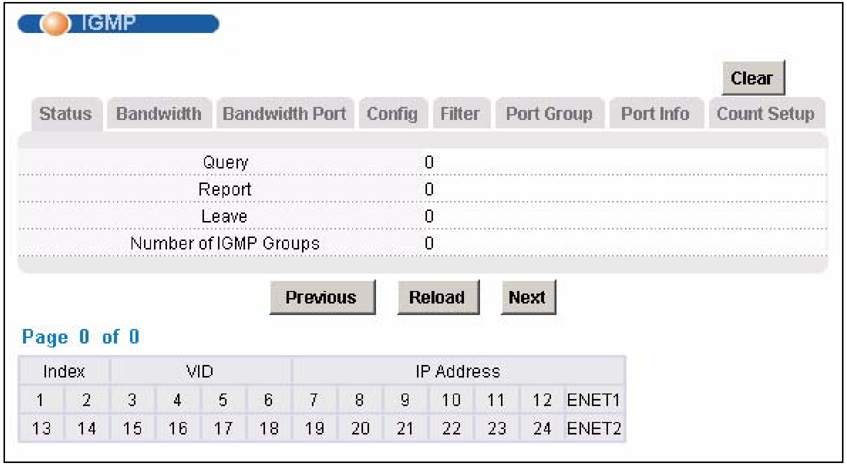
In daisychain mode, Ethernet interface 1 is set as the upstream interface and Ethernet interface 2 and the DSL ports are set as downstream interfaces.

21.3 IGMP Status Screen

Use this screen to view current IGMP information.

To open this screen, click **Advanced Application** > **IGMP**.

Figure 69 IGMP (Status)



Query	0
Report	0
Leave	0
Number of IGMP Groups	0

Page 0 of 0

Index		VID				IP Address						
1	2	3	4	5	6	7	8	9	10	11	12	ENET1
13	14	15	16	17	18	19	20	21	22	23	24	ENET2

The following table describes the labels in this screen.

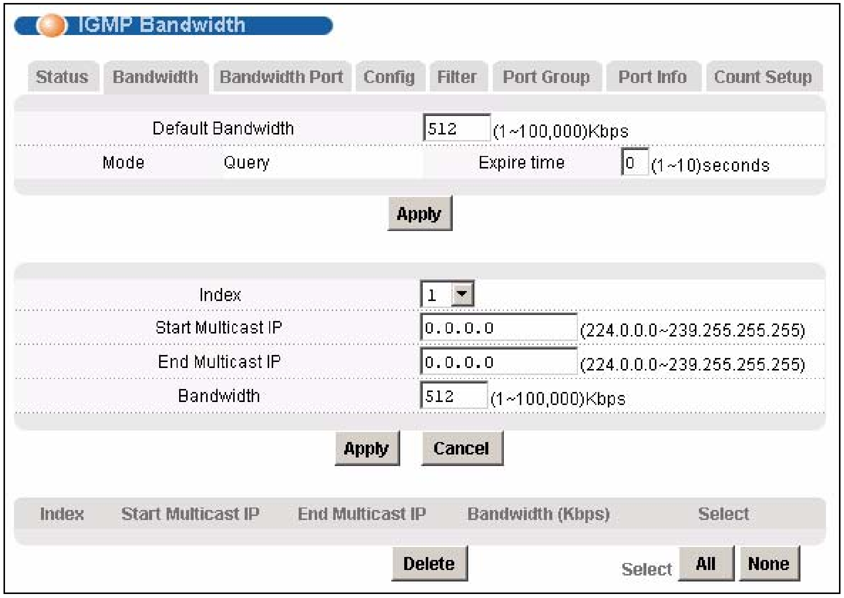
Table 34 IGMP (Status)

LABEL	DESCRIPTION
Clear	Click **Clear** to delete the information the IP DSLAM has learned about multicast groups. This resets every counter in this screen.
Query	This is the total number of Query packets received.
Report	This is the total number of Report packets received.
Leave	This is the total number of Leave packets received.
Number of IGMP Groups	This is how many IGMP groups the IP DSLAM has identified on the local network.
Previous Next	Click one of these buttons to show the previous/next screen if all of the information cannot be seen in one screen.
Reload	Click this button to refresh the screen.
Page X of X	This identifies which page of information is displayed and the total number of pages of information.
	The first table displays the names of the fields. The subsequent tables show the settings of the IGMP groups.
Index	This is the IGMP group index number.
VID	The VID is the VLAN ID on which the IGMP group is created.
IP Address	This is the IP address of an IGMP multicast group member.
1~48, enet1, enet2	These columns display the ports that are members of the IGMP snooping group.

21.4 IGMP Bandwidth Screen

Use this screen to set up bandwidth requirements for multicast channels. To open this screen, click **Advanced Application** > **IGMP** > **Bandwidth**.

Figure 70   IGMP Bandwidth



Default Bandwidth 512 (1~100,000)Kbps

Mode Query

Expire time 0 (1~10)seconds

Index 1

Start Multicast IP 0.0.0.0 (224.0.0.0~239.255.255.255)

End Multicast IP 0.0.0.0 (224.0.0.0~239.255.255.255)

Bandwidth 512 (1~100,000)Kbps

Index	Start Multicast IP	End Multicast IP	Bandwidth (Kbps)	Select

Select All None

The following table describes the labels in this screen.

Table 35   IGMP Bandwidth

LABEL	DESCRIPTION
Default Bandwidth	Enter the default bandwidth for multicast channels for which you have not configured bandwidth requirements.
Apply	Click **Apply** to save your changes to the IP DSLAM’s volatile memory. The IP DSLAM loses these changes if it is turned off or loses power, so use the **Config Save** link on the navigation panel to save your changes to the non-volatile memory when you are done configuring.
Index	Select a unique number for this setting. If you select a number that is already used, the new setting overwrites the old one when you click **Apply**.
Start Multicast IP	Enter the beginning of the multicast range.
End Multicast IP	Enter the end of the multicast range. For one multicast address, enter the start of the multicast range again.
Bandwidth	Enter the bandwidth requirement for the specified multicast range.
Apply	Click **Apply** to save the filter settings. The settings then display in the summary table at the bottom of the screen. Clicking **Apply** saves your changes to the IP DSLAM’s volatile memory. The IP DSLAM loses these changes if it is turned off or loses power, so use the **Config Save** link on the navigation panel to save your changes to the non-volatile memory when you are done configuring.
Cancel	Click **Cancel** to begin configuring the fields afresh.
	This table shows the multicast range settings.
Index	This field displays the number that identifies this setting.
Start Multicast IP	This field displays the beginning of the multicast range.
End Multicast IP	This field displays the end of the multicast range.
Bandwidth	This field displays the allowed bandwidth for the specified multicast range.
Select	Select this, and click **Delete** to remove the setting.

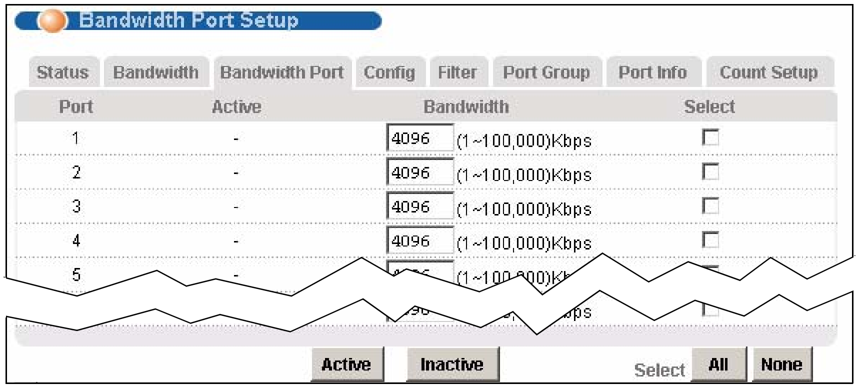
Table 35 IGMP Bandwidth (continued)

LABEL	DESCRIPTION
Delete	Click this to remove the selected settings.
Select All	Click this to select all entries in the table.
Select None	Click this to un-select all entries in the table.

21.5 Bandwidth Port Setup Screen

Use this screen to set up multicast bandwidth requirements for specific ports. To open this screen, click **Advanced Application** > **IGMP** > **Bandwidth Port**.

Figure 71 Bandwidth Port Setup



Port	Active	Bandwidth	Select
1	-	4096 (1~100,000)Kbps	□
2	-	4096 (1~100,000)Kbps	□
3	-	4096 (1~100,000)Kbps	□
4	-	4096 (1~100,000)Kbps	□
5	-		

The following table describes the labels in this screen.

Table 36 Bandwidth Port Setup

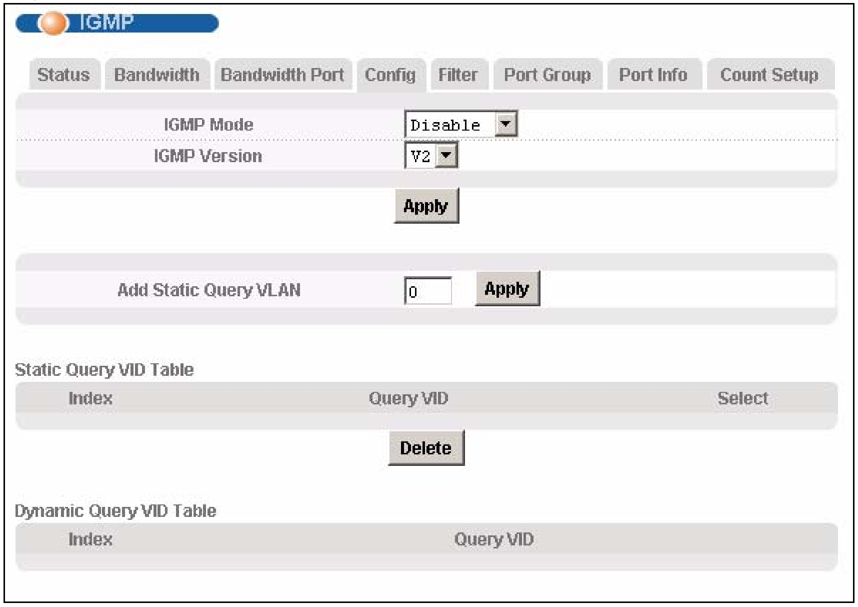
LABEL	DESCRIPTION
Port	This field shows each xDSL port number.
Active	This field shows whether or not multicast bandwidth requirements are enabled on this port. “V” displays if it is enabled and “-“ displays if it is disabled.
Bandwidth	Enter the maximum acceptable multicast bandwidth for this port. This has no effect if bandwidth requirements are disabled.
Select	Select this, and click **Active** or **Inactive** to enable or disable the specified multicast bandwidth requirements on this port.
Active	Click this to enable the specified multicast bandwidth requirements on the selected port.
Inactive	Click this to disable the specified multicast bandwidth requirements on the selected port.
Select All	Click this to select all entries in the table.
Select None	Click this to un-select all entries in the table.

21.6 Config Screen

Use this screen to configure your IGMP settings.

To open this screen, click **Advanced Application** > **IGMP** > **Config**.

Figure 72 IGMP Config



IGMP Mode: Disable

IGMP Version: V2

Add Static Query VLAN: 0

Static Query VID Table

Index	Query VID	Select

Dynamic Query VID Table

Index	Query VID

The following table describes the labels in this screen.

Table 37 IGMP Config

LABEL	DESCRIPTION
IGMP Mode	Select **Proxy** to have the device use IGMP proxy. Select **Snooping** to have the device passively learn multicast groups. Select **Disable** to have the device not use either IGMP proxy or snooping.
IGMP Version	Select which version of IGMP you want the device to support. Select IGMPv2 (**V2**) or IGMPv3 (**V3**). If you select IGMPv2, the device discards IGMPv3 packets. This provides better security if none of the devices in the network use IGMPv3. If you select IGMPv3, the device recognizes both IGMPv2 and IGMPv3.
Apply	Click **Apply** to save your IGMP mode settings. Clicking **Apply** saves your changes to the IP DSLAM's volatile memory. The IP DSLAM loses these changes if it is turned off or loses power, so use the **Config Save** link on the navigation panel to save your changes to the non-volatile memory when you are done configuring.
Add Static Query VLAN	Type the number for an IGMP proxy VLAN and click **Apply** to add a static VLAN on which the system sends IGMP query messages. This should be the number of a subscriber VLAN. The VLAN will appear in the **Static Query VID Table**. You must configure the system's VLAN settings before you can set static query VIDs.
Static Query VID Table	This table lists the manually added VLANs on which the system sends IGMP query messages. These are multicast service subscriber VLANs.
Index	This is the index number of an entry.
Query VID	This field displays a query VLAN which has manually added.
Select, Delete	Select an entry and click **Delete** to remove it from the table.

Table 37 IGMP Config (continued)

LABEL	DESCRIPTION
Dynamic Query VID Table	This table lists the IGMP query VLANs that the system has dynamically learned via IGMP snooping or IGMP proxy. These are VLANs on which the system sends IGMP query messages. They are multicast service subscriber VLANs.
Index	This is the index number of an entry.
Query VID	This field displays a query VLAN which has dynamically learned.

21.7 IGMP Filter Profile Screen

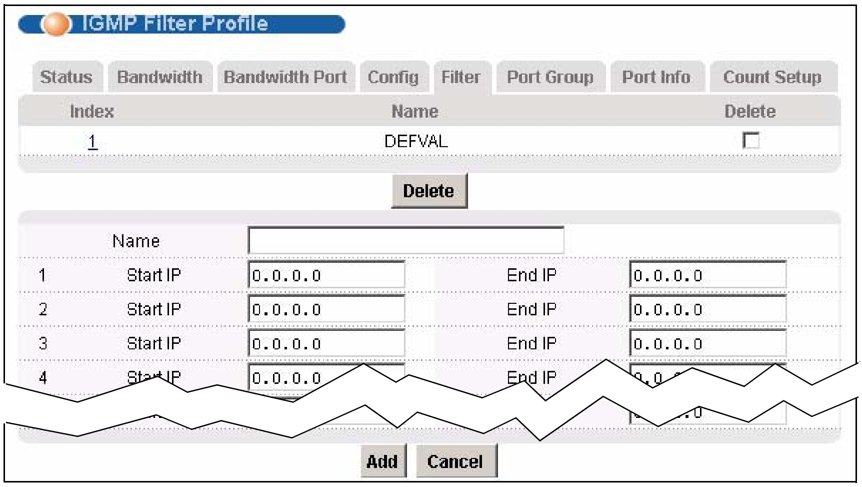
To open this screen, click **Advanced Application** > **IGMP** > **Filter**.

You can use the IGMP filter profiles to control access to a service that uses a specific multicast group (like a SIP server for example). Configure an IGMP filter profile that allows access to that multicast group. Then assign the IGMP filter profile to xDSL ports that are allowed to use the service.

The **DEFVAL** IGMP filter profile is assigned to all of the xDSL ports by default. It allows a port to join all multicast IP addresses (224.0.0.0~239.255.255.255). If you want to allow a xDSL subscriber access to only specific IGMP multicast groups, use the **IGMP Filter Profile** screen to configure a different profile and then assign it to the subscriber's xDSL port in the **XDSL Port Setting** screen (see Section 16.9.1 on page 106).

The top of the screen displays the configured IGMP filter profiles. Use the bottom part of the screen (with the **Add** and **Cancel** buttons) to add or edit alarm profiles.

Figure 73 IGMP Filter Profile



Index	Name	Delete
1	DEFVAL	□

Name

1	Start IP	0.0.0.0	End IP	0.0.0.0
2	Start IP	0.0.0.0	End IP	0.0.0.0
3	Start IP	0.0.0.0	End IP	0.0.0.0
4	Start IP	0.0.0.0	End IP	0.0.0.0

The following table describes the labels in this screen.

Table 38 IGMP Filter Profile

LABEL	DESCRIPTION
Index	This is the number of the IGMP filter profile. Click a profile's index number to edit the profile. You cannot edit the **DEFVAL** profile.
Name	This name identifies the IGMP filter profile.

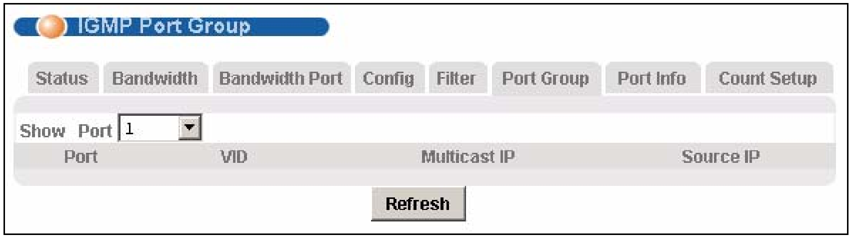
Table 38 IGMP Filter Profile (continued)

LABEL	DESCRIPTION
Delete	Select the **Delete** check box and click **Delete** to remove an IGMP filter profile. You cannot delete the **DEFVAL** profile.
Name	Type a name to identify the IGMP filter profile (you cannot change the name of the DEFVAL profile). You can use up to 31 ASCII characters; spaces are not allowed.
Start IP	Enter the starting multicast IP address for a range of multicast IP addresses to which you want this IGMP filter profile to allow access.
End IP	Enter the ending multicast IP address for a range of IP addresses to which you want this IGMP filter profile to allow access. If you want to add a single multicast IP address, enter it in both the **Start IP** and **End IP** fields.
Add	Click **Add** to save your changes to the IP DSLAM's volatile memory. The IP DSLAM loses these changes if it is turned off or loses power, so use the **Config Save** link on the navigation panel to save your changes to the non-volatile memory when you are done configuring.
Cancel	Click **Cancel** to start configuring the screen again.

21.8 IGMP Port Group Screen

Use this screen to display the current list of multicast groups each port joins. To open this screen, click **Advanced Application** > **IGMP** > **Port Group**.

Figure 74 IGMP Port Group



The following table describes the labels in this screen.

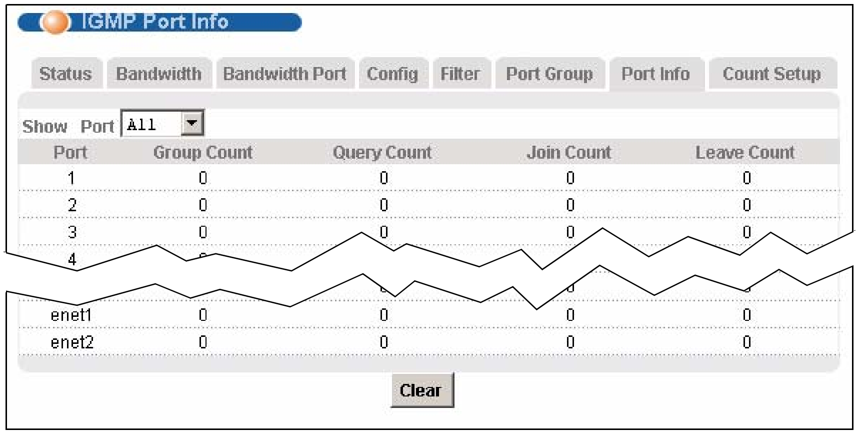
Table 39 IGMP Port Group

LABEL	DESCRIPTION
Show Port	Select a port for which you wish to view information.
Port	This field shows each port number.
VID	This field shows the associated VLAN ID.
Multicast IP	This field shows the IP address of the multicast group joined by this port.
Source IP	This field shows the IP address of the client that joined the multicast group on this port.
Refresh	Click **Refresh** to display updated information.

21.9 IGMP Port Info Screen

Use this screen to display the current number of IGMP-related packets received on each port. To open this screen, click **Advanced Application** > **IGMP** > **Port Info**.

Figure 75 IGMP Port Info



Show Port All

Port	Group Count	Query Count	Join Count	Leave Count
1	0	0	0	0
2	0	0	0	0
3	0	0	0	0
4				
enet1	0	0	0	0
enet2	0	0	0	0

The following table describes the labels in this screen.

Table 40 IGMP Port Info

LABEL	DESCRIPTION
Show Port	Select a port for which you wish to view information.
Port	This field shows each port number.
Group Count	This is the total number of Group packets received on this port.
Query Count	This is the total number of Query packets received on this port.
Join Count	This is the total number of Join packets received on this port.
Leave Count	This is the total number of Leave packets received on this port.
Clear	Click **Clear** to delete the information the IP DSLAM has learned about multicast groups. This resets every counter in this screen.

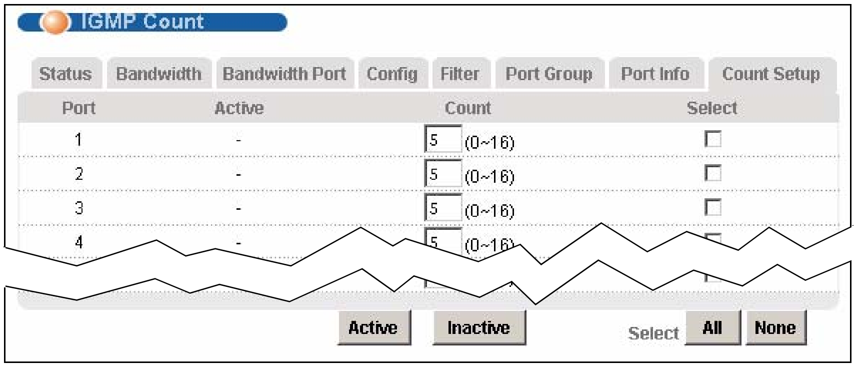
21.10 IGMP Count Screen

Use this screen to limit the number of IGMP groups a subscriber on a port can join. This allows you to control the distribution of multicast services (such as content information distribution) based on service plans and types of subscription.

IGMP count is useful for ensuring the service quality of high bandwidth services like video or Internet Protocol television (IPTV). IGMP count can limit how many channels (IGMP groups) the subscriber connected to an xDSL port can use at a time. If each channel requires 4~5 Mbps of download bandwidth, and the subscriber’s connection supports 11 Mbps, you can use IGMP count to limit the subscriber to using just 2 channels at a time. This also effectively limits the subscriber to using only two IPTVs with the xDSL connection.

To open this screen, click **Advanced Application** > **IGMP** > **Counts Setup**.

Figure 76 IGMP Count



Port	Active	Count	Select
1	-	5 (0~16)	□
2	-	5 (0~16)	□
3	-	5 (0~16)	□
4	-	5 (0~16)	□

The following table describes the labels in this screen.

Table 41 IGMP Counts

LABEL	DESCRIPTION
Port	This field shows each xDSL port number.
Active	This field shows whether or not the IGMP count limit is enabled on this port. “V” displays if it is enabled and “-“ displays if it is disabled.
Count	Enter the maximum number of IGMP groups a subscriber on this port can join. This has no effect if the IGMP count limit is disabled.
Select	Select this, and click **Active** or **Inactive** to enable or disable the specified IGMP count limit on this port.
Active	Click this to enable the specified IGMP count limits on the selected ports.
Inactive	Click this to disable the specified IGMP count limits on the selected ports.
Select All	Click this to select all entries in the table.
Select None	Click this to un-select all entries in the table.

22

Static Multicast

This chapter describes the **Static Multicast** screen.

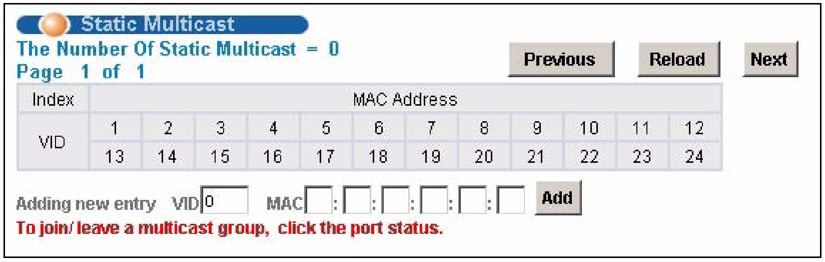
22.1 Static Multicast

Use static multicast to allow incoming frames based on multicast MAC address(es) that you specify. This feature can be used in conjunction with IGMP snooping/proxy to allow multicast MAC address(es) that are not learned by IGMP snooping or IGMP proxy. Use static multicast to pass routing protocols, such as RIP and OSPF.

22.2 Static Multicast Screen

To open this screen, click **Advanced Application** > **Static Multicast**.

Figure 77 Static Multicast



Static Multicast

The Number Of Static Multicast = 0

Page 1 of 1

Index	MAC Address											
VID	1	2	3	4	5	6	7	8	9	10	11	12
	13	14	15	16	17	18	19	20	21	22	23	24

Adding new entry VID 0 MAC : : : : :

To join/ leave a multicast group, click the port status.

The following table describes the labels in this screen.

Table 42 Static Multicast

LABEL	DESCRIPTION
The Number of Static Multicast	This is the number of static multicast entries configured on the IP DSLAM.
Page X of X	This identifies which page of information is displayed and the total number of pages of information.
Previous Next	Click one of these buttons to show the previous/next screen if all status information cannot be seen in one screen.
Reload	Click this button to refresh the screen.
	The first table displays the names of the fields. The subsequent tables show the settings of the IGMP groups.
Index	This is the static multicast group index number.
MAC Address	This is the multicast MAC address.

Table 42 Static Multicast (continued)

LABEL	DESCRIPTION
1~24	These fields display the static multicast group membership status of the xDSL ports. “V” displays for members and “-“ displays for non-members. Click an xDSL port’s status to change it (clicking a “V” changes it to “-“ and vise versa).
Join All	Click **Join All** to make all of the xDSL ports members of the static multicast group.
Leave All	Click **Leave All** to remove all of the xDSL ports from the static multicast group.
Delete	Click **Delete** to remove a static multicast group.
Adding new entry Add	Type a multicast MAC address in the field, and click the **Add** button to create a new static multicast entry. Multicast MAC addresses must be `01:00:5E:xx:xx:xx`, where `x` is a “don’t care” value. For example, `01:00:5E:10:10:10` is a valid multicast MAC address. Clicking **Add** saves your changes to the IP DSLAM’s volatile memory. The IP DSLAM loses these changes if it is turned off or loses power, so use the **Config Save** link on the navigation panel to save your changes to the non-volatile memory when you are done configuring.

23

Multicast VLAN

This chapter describes the **Multicast VLAN** screens.

23.1 Multicast VLAN Overview

Multicast VLAN allows one single multicast VLAN to be shared among different subscriber VLANs on the network. This improves bandwidth utilization by reducing multicast traffic in the subscriber VLANs and simplifies multicast group management.

When the IP DSLAM forwards traffic to a subscriber port, it tries to forward traffic to a normal PVC with the same VLAN ID. If this PVC does not exist, the IP DSLAM uses the super channel instead. This applies to all downstream traffic, not just multicast traffic.

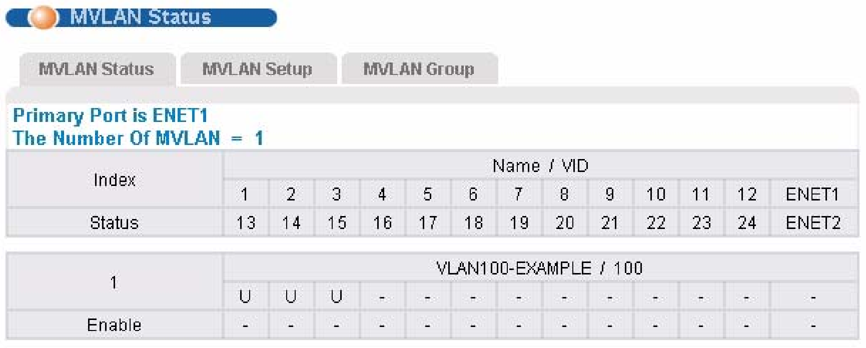
It is suggested to use a super channel for multicast VLAN. If a normal PVC is used and the multicast VLAN ID is not the same as the PVC's VID, the IP DSLAM does not forward traffic to this PVC even if the subscriber's port has joined the multicast VLAN.

Since the IP DSLAM might change the subscriber's VLAN ID to the multicast VLAN ID, both the subscriber's port and the Ethernet port should join the multicast VLAN.

23.2 MVLAN Status Screen

Use this screen to look at a summary of all multicast VLAN on the IP DSLAM. To open this screen, click **Advanced Application > Multicast VLAN**.

Figure 78 MVLAN Status



Primary Port is ENET1
The Number Of MVLAN = 1

Index	Name / VID												
	1	2	3	4	5	6	7	8	9	10	11	12	ENET1
Status	13	14	15	16	17	18	19	20	21	22	23	24	ENET2
1	VLAN100-EXAMPLE / 100												
	U	U	U	-	-	-	-	-	-	-	-	-	-
Enable	-	-	-	-	-	-	-	-	-	-	-	-	-

The following table describes the labels in this screen.

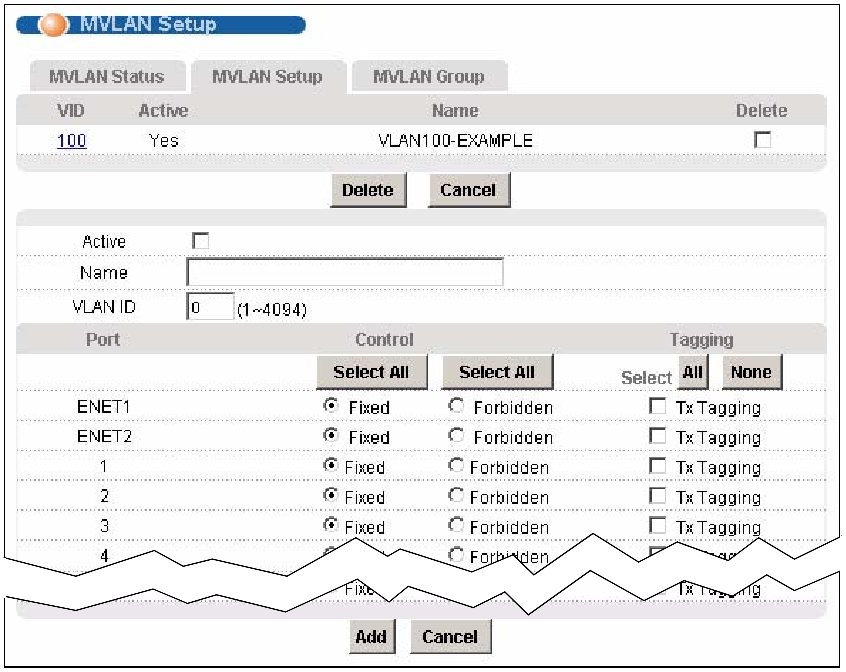
Table 43 MVLAN Status

LABEL	DESCRIPTION
The Number of MVLAN	This is the number of multicast VLAN configured on the IP DSLAM.
	The first table displays the names of the fields. The subsequent tables show the settings for each multicast VLAN.
Index	This is a sequential value and is not associated with this multicast VLAN.
Name / VID	This field shows the name and VLAN ID of this multicast VLAN.
1~24 ENET1-2	These fields display whether or not each port is a member of this multicast VLAN. “V” displays for members and “-“ displays for non-members. You can change these settings in the **MVLAN Setup** screen.
Status	This field shows whether this multicast VLAN is active (**Enable**) or inactive (**Disable**).

23.3 MVLAN Setup Screen

Use this screen to configure basic settings and port members for each multicast VLAN. To open this screen, click **Advanced Application** > **Multicast VLAN** > **MVLAN Setup**.

Figure 79 MVLAN Setup



VID	Active	Name	Delete
100	Yes	VLAN100-EXAMPLE	□

Active	□
Name	
VLAN ID	0 (1~4094)

Port	Control		Tagging
ENET1	● Fixed	○ Forbidden	□ Tx Tagging
ENET2	● Fixed	○ Forbidden	□ Tx Tagging
1	● Fixed	○ Forbidden	□ Tx Tagging
2	● Fixed	○ Forbidden	□ Tx Tagging
3	● Fixed	○ Forbidden	□ Tx Tagging
4		○ Forbidden	

The following table describes the labels in this screen.

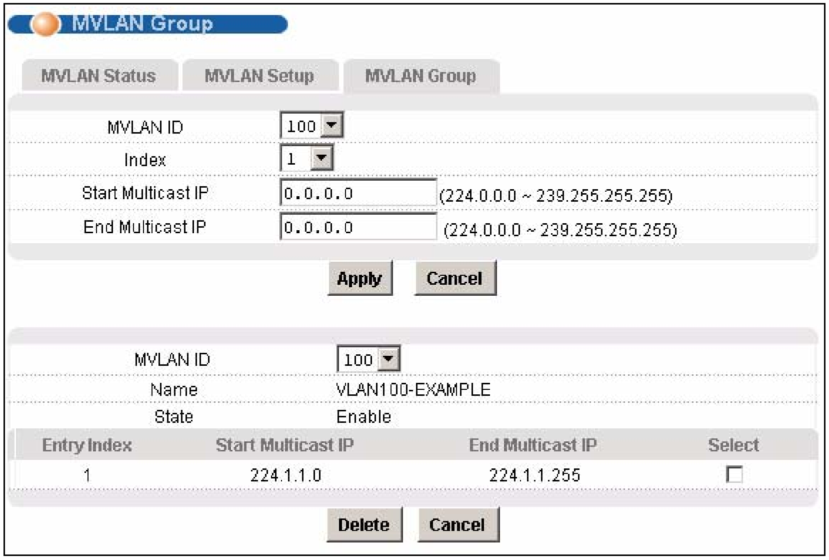
Table 44 MVLAN Setup

LABEL	DESCRIPTION
VID	This field shows the VLAN ID of each multicast VLAN. Click it to edit its basic settings and port members in the fields below.
Active	This field shows whether this multicast VLAN is active (**Yes**) or inactive (**No**).
Name	This field shows the name of this multicast VLAN.
Delete	Select the check boxes of the rule(s) that you want to remove in the **Delete** column and then click the **Delete** button. You cannot delete a VLAN if any PVIDs are set to use the VLAN or the VLAN is the CPU (management) VLAN.
Cancel	Click **Cancel** to begin configuring the fields afresh.
Active	Select this if you want the multicast VLAN to be active. Clear this if you want the multicast VLAN to be inactive.
Name	Enter a descriptive name for the multicast VLAN. The name can be 1-31 printable ASCII characters long. Spaces are not allowed.
VLAN ID	Enter the VLAN ID of the multicast VLAN; the valid range is between 1 and 4094.
Port	This field displays each port number.
Control	Select **Fixed** for the port to be a permanent member of this multicast VLAN. Use the **Select All** button to include every port. Select **Forbidden** if you want to prohibit the port from joining this multicast VLAN. Use the **Select All** button to include every port.
Tagging	Select **TX Tagging** if you want the port to tag all outgoing frames transmitted with this VLAN ID. Use the **All** button to include every port. Use the **None** button to clear all of the ports check boxes.
Add	Click **Add** to save your changes to the IP DSLAM’s volatile memory. The IP DSLAM loses these changes if it is turned off or loses power, so use the **Config Save** link on the navigation panel to save your changes to the non-volatile memory when you are done configuring.
Cancel	Click **Cancel** to begin configuring the fields afresh.

23.4 MVLAN Group Screen

Use this screen to configure ranges of multicast IP addresses for each multicast VLAN. To open this screen, click **Advanced Application** > **Multicast VLAN** > **MVLAN Group**.

Figure 80 MVLAN Group



MVLAN ID	100
Index	1
Start Multicast IP	0.0.0.0 (224.0.0.0 ~ 239.255.255.255)
End Multicast IP	0.0.0.0 (224.0.0.0 ~ 239.255.255.255)

MVLAN ID	100
Name	VLAN100-EXAMPLE
State	Enable

Entry Index	Start Multicast IP	End Multicast IP	Select
1	224.1.1.0	224.1.1.255	□

The following table describes the labels in this screen.

Table 45 MVLAN Group

LABEL	DESCRIPTION
MVLAN ID	Select the VLAN ID of the multicast VLAN for which you want to configure a range of multicast IP addresses.
Index	Select the index number of the multicast VLAN group (the range of multicast IP addresses) you want to configure for this multicast VLAN. If you want to change the current settings, select an index number that already exists. If you want to add a new multicast VLAN group, select an index number that does not exist.
Start Multicast IP	Enter the beginning of the range of multicast IP addresses. The IP address must be a valid multicast IP address, between 224.0.0.0 and 239.255.255.255.
End Multicast IP	Enter the end of the range of multicast IP addresses. The IP address must be a valid multicast IP address, between 224.0.0.0 and 239.255.255.255.
Apply	Click **Apply** to save your changes to the IP DSLAM’s volatile memory. The IP DSLAM loses these changes if it is turned off or loses power, so use the **Config Save** link on the navigation panel to save your changes to the non-volatile memory when you are done configuring.
Cancel	Click **Cancel** to begin configuring the fields afresh.
MVLAN ID	Select the VLAN ID of the multicast VLAN for which you want to look at or remove the multicast IP addresses currently added to it.
Name	This field displays the name of this multicast VLAN.
State	This field shows whether this multicast VLAN is active (**Enable**) or inactive (**Disable**).
Entry Index	This field displays the index number of each multicast VLAN group (the range of multicast IP addresses) configured for this multicast VLAN.
Start Multicast IP	This field displays the beginning of this range of multicast IP addresses.
End Multicast IP	This field displays the end of this range of multicast IP addresses.
Select	Select this, and click **Delete** to remove the multicast VLAN group.
Delete	Click this to remove the selected multicast VLAN groups.
Cancel	Click **Cancel** to begin configuring the fields afresh.

24

Packet Filtering

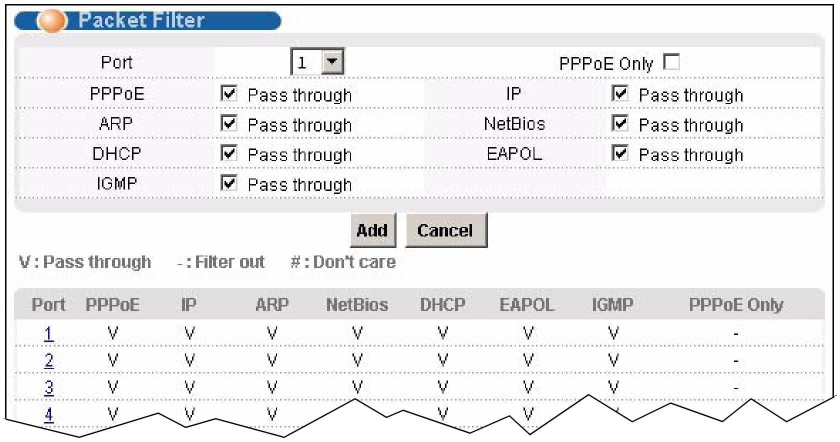
This chapter describes how to configure the **Packet Filter** screen.

24.1 Packet Filter Screen

Use this screen to set which types of packets the IP DSLAM accepts on individual xDSL ports.

To open this screen, click **Advanced Application** > **Filtering**.

Figure 81 Packet Filter



Packet Filter

Port	1	PPPoE Only	□
PPPoE	☑ Pass through	IP	☑ Pass through
ARP	☑ Pass through	NetBios	☑ Pass through
DHCP	☑ Pass through	EAPOL	☑ Pass through
IGMP	☑ Pass through		

V : Pass through - : Filter out # : Don't care

Port	PPPoE	IP	ARP	NetBios	DHCP	EAPOL	IGMP	PPPoE Only
1	V	V	V	V	V	V	V	-
2	V	V	V	V	V	V	V	-
3	V	V	V	V	V	V	V	-
4	V	V	V		V	V		

The following table describes the labels in this screen.

Table 46 Packet Filter

LABEL	DESCRIPTION
Port	Use this drop-down list box to select an xDSL port for which you wish to configure packet type filtering. This box is read-only after you click on one of the port numbers in the table below.
PPPoE Only	Select this to allow only PPPoE traffic. This will gray out the check boxes for other packet types and the system will drop any non-PPPoE packets.
	Select the check boxes of the types of packets to accept on the xDSL port. When you clear one of these check boxes, the field label changes to **Filter Out** and the system drops the corresponding type of packets
PPPoE Pass through	Point-to-Point Protocol over Ethernet relies on PPP and Ethernet. It is a specification for connecting the users on an Ethernet to the Internet through a common broadband medium, such as a single xDSL line, wireless device or cable modem.
IP Pass through	Internet Protocol. The underlying protocol for routing packets on the Internet and other TCP/IP-based networks.

Table 46 Packet Filter (continued)

LABEL	DESCRIPTION
ARP Pass through	Address Resolution Protocol is a protocol for mapping an Internet Protocol address (IP address) to a physical computer address that is recognized in the local network.
NetBios Pass through	NetBIOS (Network Basic Input/Output System) are TCP or UDP packets that enable a computer to find other computers.
DHCP Pass through	Dynamic Host Configuration Protocol automatically assigns IP addresses to clients when they log on. DHCP centralizes IP address management on central computers that run the DHCP server program. DHCP leases addresses, for a period of time, which means that past addresses are “recycled” and made available for future reassignment to other systems.
EAPOL Pass through	EAP (Extensible Authentication Protocol, RFC 2486) over LAN. EAP is used with IEEE 802.1x to allow additional authentication methods (besides RADIUS) to be deployed with no changes to the access point or the wireless clients.
IGMP Pass through	Internet Group Multicast Protocol is used when sending packets to a specific group of hosts.
Add	Click **Add** to save the filter settings. The settings then display in the summary table at the bottom of the screen. Clicking **Add** saves your changes to the IP DSLAM’s volatile memory. The IP DSLAM loses these changes if it is turned off or loses power, so use the **Config Save** link on the navigation panel to save your changes to the non-volatile memory when you are done configuring.
Cancel	Click **Cancel** to begin configuring the fields afresh.
	This table shows the xDSL port packet filter settings.
Port	These are the numbers of the xDSL ports. Click this number to edit the port’s filter settings in the section at the top.
PPPoE, IP, ARP, NetBios, DHCP, EAPOL, IGMP, PPPoE Only	These are the packet filter settings for each port. “**V**” displays for the packet types that the IP DSLAM is to accept on the port. “**-**“ displays for packet types that the IP DSLAM is to reject on the port (packet types that are not listed are accepted). When you select **PPPoE Only**,”**#**” appears for all of the packet types. With **PPPoE Only**, the IP DSLAM rejects all packet types except for PPPoE (packet types that are not listed are also rejected).

25

MAC Filter

This chapter introduces the MAC filter.

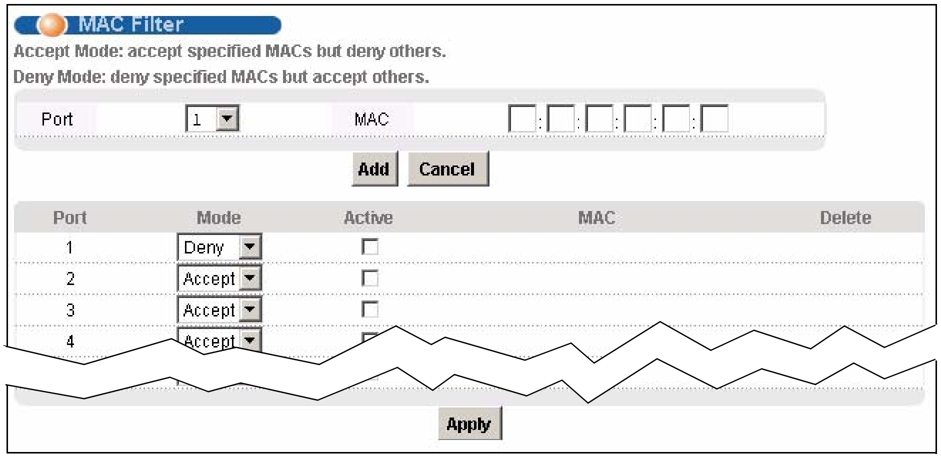
25.1 MAC Filter Introduction

Use the MAC filter to control from which MAC (Media Access Control) addresses frames can (or cannot) come in through a port.

25.2 MAC Filter Screen

To open this screen, click **Advanced Application** > **MAC Filter**.

Figure 82 MAC Filter



Accept Mode: accept specified MACs but deny others.

Deny Mode: deny specified MACs but accept others.

Port 1 MAC □:□:□:□:□:□

Port	Mode	Active	MAC	Delete
1	Deny	□		
2	Accept	□		
3	Accept	□		
4	Accept	□		

The following table describes the labels in this screen.

Table 47 MAC Filter

LABEL	DESCRIPTION
Port	Use this drop-down list box to select an xDSL port for which you wish to configure MAC filtering.
MAC	Type a device’s MAC address in hexadecimal notation (xx:xx:xx:xx:xx:xx, where x is a number from 0 to 9 or a letter from a to f) in this field. The MAC address must be a valid MAC address.

Table 47 MAC Filter (continued)

LABEL	DESCRIPTION
Add	Click **Add** to save your changes to the IP DSLAM's volatile memory. The IP DSLAM loses these changes if it is turned off or loses power, so use the **Config Save** link on the navigation panel to save your changes to the non-volatile memory when you are done configuring.
Cancel	Click **Cancel** to begin configuring this screen afresh.
Port	These are the numbers of the xDSL ports.
Mode	Select **Accept** to only allow frames from MAC addresses that you specify and block frames from other MAC addresses. Select **Deny** to block frames from MAC addresses that you specify and allow frames from other MAC addresses.
Active	Select this check box to turn on MAC filtering for a port.
MAC	This field lists the MAC addresses that are set for this port.
Delete	Click **Delete** to remove a MAC address from the list.
Apply	Click **Apply** to save your changes to the IP DSLAM's volatile memory. The IP DSLAM loses these changes if it is turned off or loses power, so use the **Config Save** link on the navigation panel to save your changes to the non-volatile memory when you are done configuring.

26

Rapid Spanning Tree Protocol

This chapter introduces the Spanning Tree Protocol (STP) and Rapid Spanning Tree Protocol (RSTP).

26.1 RSTP and STP

RSTP adds rapid reconfiguration capability to STP. The IP DSLAM supports RSTP and the earlier STP. RSTP and STP detect and break network loops and provide backup links between switches, bridges or routers. They allow a device to interact with other RSTP or STP-aware devices in your network to ensure that only one path exists between any two stations on the network. The Integrated Ethernet Switch uses RSTP by default but can still operate with STP switches (although without RSTP's benefits).

The root bridge is the base of the spanning tree. Path cost is the cost of transmitting a frame onto a LAN through that port. It is assigned according to the speed of the link to which a port is attached. The slower the media, the higher the cost, as illustrated in the following table.

Table 48 Path Cost

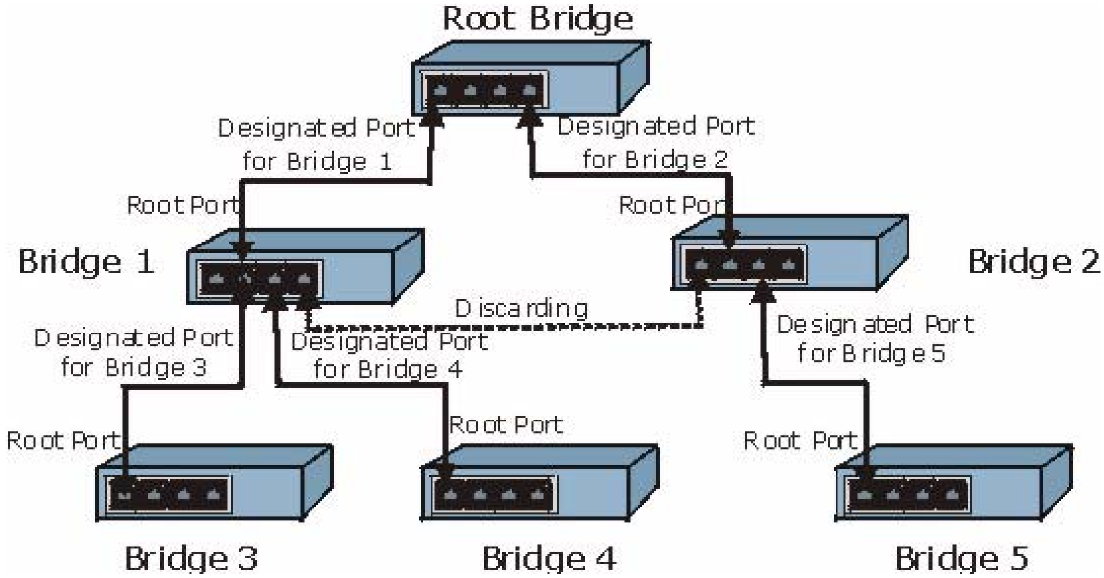
	LINK SPEED	RECOMMENDED VALUE	RECOMMENDED RANGE	ALLOWED RANGE
Path Cost	4Mbps	250	100 to 1000	1 to 65535
Path Cost	10Mbps	100	50 to 600	1 to 65535
Path Cost	16Mbps	62	40 to 400	1 to 65535
Path Cost	100Mbps	19	10 to 60	1 to 65535
Path Cost	1Gbps	4	3 to 10	1 to 65535
Path Cost	10Gbps	2	1 to 5	1 to 65535

On each bridge, the root port is the port through which this bridge communicates with the root. It is the port on this Integrated Ethernet Switch with the lowest path cost to the root (the root path cost). If there is no root port, then this Integrated Ethernet Switch has been accepted as the root bridge of the spanning tree network.

For each LAN segment, a designated bridge is selected. This bridge has the lowest cost to the root among the bridges connected to the LAN.

After a bridge determines the lowest cost-spanning tree with RSTP, it enables the root port and the ports that are the designated ports for the connected LANs, and disables all other ports that participate in RSTP. Network packets are therefore only forwarded between enabled ports, eliminating any possible network loops.

Figure 83 STP Root Ports and Designated Ports


Root Bridge
Designated Port for Bridge 1
Designated Port for Bridge 2
Root Port
Root Port
Bridge 1
Bridge 2
Discarding
Designated Port for Bridge 3
Designated Port for Bridge 4
Designated Port for Bridge 5
Root Port
Root Port
Root Port
Bridge 3
Bridge 4
Bridge 5

RSTP-aware devices exchange Bridge Protocol Data Units (BPDUs) periodically. When the bridged LAN topology changes, a new spanning tree is constructed.

In RSTP, the devices send BPDUs every Hello Time. If an RSTP-aware device does not get a Hello BPDU after three Hello Times pass (or the Max Age), the device assumes that the link to the neighboring bridge is down. This device then initiates negotiations with other devices to reconfigure the network to re-establish a valid network topology.

In STP, once a stable network topology has been established, all devices listen for Hello BPDUs transmitted from the root bridge. If an STP-aware device does not get a Hello BPDU after a predefined interval (Max Age), the device assumes that the link to the root bridge is down. This device then initiates negotiations with other devices to reconfigure the network to re-establish a valid network topology.

RSTP assigns three port states to eliminate packet looping while STP assigns five (see Table 49 on page 162). A device port is not allowed to go directly from blocking state to forwarding state so as to eliminate transient loops.

Table 49 RSTP Port States

RSTP PORT STATE	STP PORT STATE	DESCRIPTION
Discarding	Disabled	RSTP or STP is disabled (default).
Discarding	Blocking	In RSTP, BPDUs are discarded. In STP, only configuration and management BPDUs are received and processed.
Discarding	Listening	In RSTP, BPDUs are discarded. In STP, all BPDUs are received and processed.
Learning	Learning	All BPDUs are received and processed. Information frames are submitted to the learning process but not forwarded.
Forwarding	Forwarding	All BPDUs are received and processed. All information frames are received and forwarded.

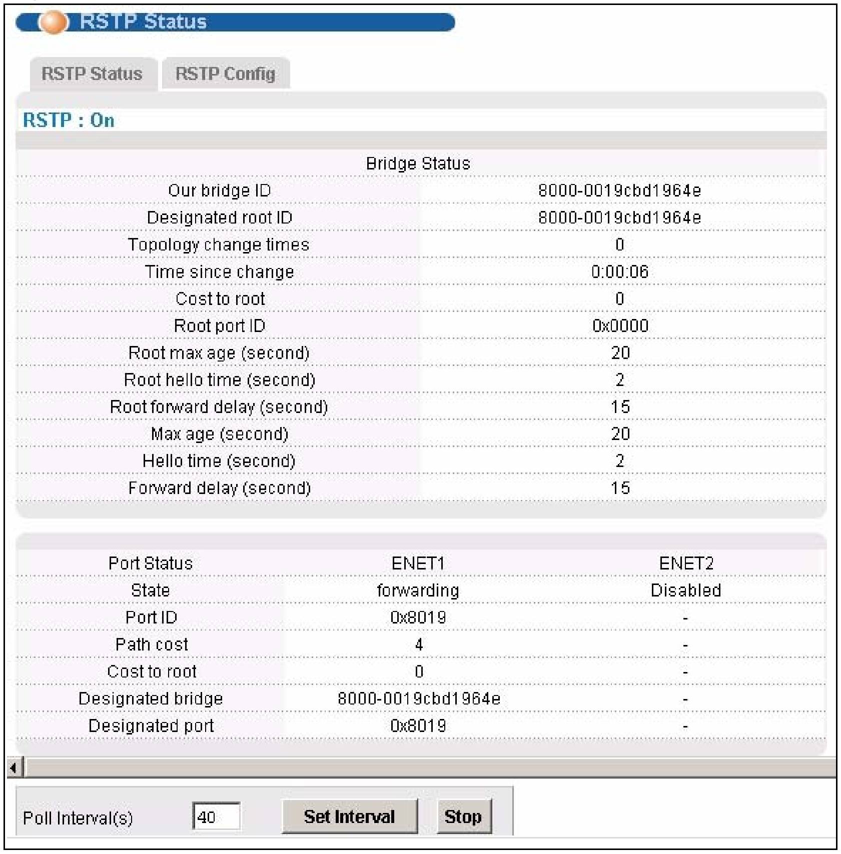
See the IEEE 802.1w standard for more information on RSTP. See the IEEE 802.1D standard for more information on STP.

You can not use the IP DSLAM as the RSTP root device.

26.2 RSTP Status Screen

To open this screen, click **Advanced Application** > **RSTP**.

Figure 84 RSTP Status



RSTP : On

Bridge Status	
Our bridge ID	8000-0019cbd1964e
Designated root ID	8000-0019cbd1964e
Topology change times	0
Time since change	0:00:06
Cost to root	0
Root port ID	0x0000
Root max age (second)	20
Root hello time (second)	2
Root forward delay (second)	15
Max age (second)	20
Hello time (second)	2
Forward delay (second)	15

Port Status	ENET1	ENET2
State	forwarding	Disabled
Port ID	0x8019	-
Path cost	4	-
Cost to root	0	-
Designated bridge	8000-0019cbd1964e	-
Designated port	0x8019	-

Poll Interval(s) 40

The following table describes the labels in this screen.

Table 50 RSTP Status

LABEL	DESCRIPTION
RSTP	This field displays **On** if RSTP is activated. Otherwise, it displays **Off**.
Bridge Status	If STP is activated, the following fields appear. If STP is not activated, **Disabled** appears.
Our bridge ID	This is the unique identifier for this bridge, consisting of bridge priority plus MAC address. This ID is the same in **Designated root ID** if the IP DSLAM is the root switch.
Designated root ID	This is the unique identifier for the root bridge, consisting of bridge priority plus MAC address. This ID is the same in **Our bridge ID** if the IP DSLAM is the root switch.

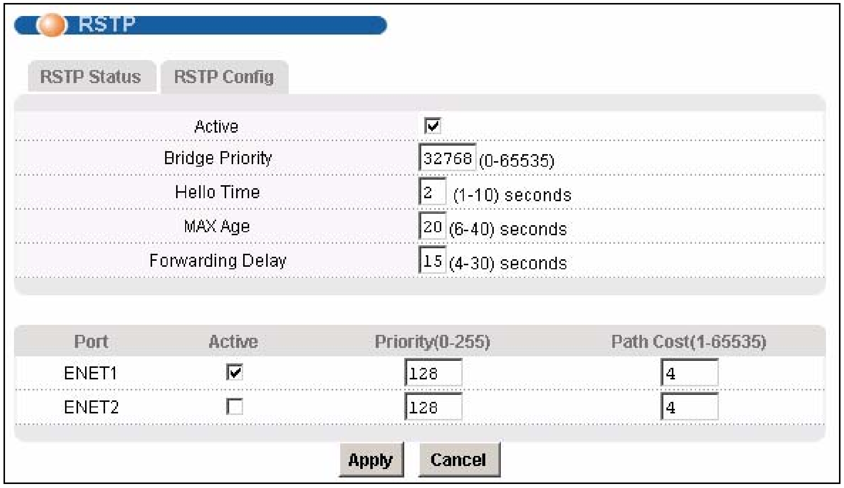
Table 50 RSTP Status (continued)

LABEL	DESCRIPTION
Topology change times	This is the number of times the spanning tree has been reconfigured.
Time since change	This is the time since the spanning tree was last reconfigured.
Cost to root	This is the path cost from the root port on this switch to the root switch.
Root port ID	This is the priority and number of the port on the switch through which this switch must communicate with the root of the Spanning Tree. “0x0000” displays when this device is the root switch.
Root max age (second)	This is the maximum time (in seconds) the root switch can wait without receiving a configuration message before attempting to reconfigure.
Root hello time (second)	This is the time interval (in seconds) at which the root switch transmits a configuration message. The root bridge determines **Hello time, Max age** and **Forwarding delay**.
Root forward delay (second)	This is the time (in seconds) the root switch will wait before changing states (that is, listening to learning to forwarding).
Max age (second)	This is the maximum time (in seconds) the IP DSLAM can wait without receiving a configuration message before attempting to reconfigure.
Hello time (second)	This is the time interval (in seconds) at which the IP DSLAM transmits a configuration message. The root bridge determines **Hello time, Max age** and **Forwarding delay**.
Forward delay (second)	This is the time (in seconds) the IP DSLAM will wait before changing states (that is, listening to learning to forwarding).
Port Status	This identifies the IP DSLAM’s ports that support the use of STP. If STP is activated, the following fields appear. If STP is not activated, **Disabled** appears.
State	This field displays the port’s RSTP (or STP) state. With RSTP, the state can be **discarding**, **learning** or **forwarding**. With STP, the state can be **disabled**, **blocking**, **listening**, **learning**, or **forwarding**. **Disabled** appears when RSTP has not been turned on for the individual port or the whole device.
Port ID	This is the priority and number of the port on the switch through which this switch must communicate with the root of the Spanning Tree. “0x0000” displays when this device is the root switch.
Path cost	This is the path cost from this port to the root switch.
Cost to root	This is the path cost from the root port on this switch to the root switch.
Designated bridge	This is the unique identifier for the bridge that has the lowest path cost to reach the root bridge, consisting of bridge priority plus MAC address.
Designated port	This is the port on the designated bridge that has the lowest path cost to reach the root bridge, consisting of bridge priority.
Poll Interval(s) Set Interval	The text box displays how often (in seconds) this screen refreshes. You may change the refresh interval by typing a new number in the text box and then clicking **Set Interval**.
Stop	Click **Stop** to halt STP statistic polling.

26.3 RSTP Config Screen

To open this screen, click **Advanced Application > RSTP** > **RSTP Config**.

Figure 85 RSTP Config



Active	☑
Bridge Priority	32768 (0-65535)
Hello Time	2 (1-10) seconds
MAX Age	20 (6-40) seconds
Forwarding Delay	15 (4-30) seconds

Port	Active	Priority(0-255)	Path Cost(1-65535)
ENET1	☑	128	4
ENET2	☐	128	4

The following table describes the labels in this screen.

Table 51 RSTP Config

LABEL	DESCRIPTION
Active	Select this check box to turn on RSTP.
Bridge Priority	Bridge priority is used in determining the root switch, root port and designated port. The switch with the highest priority (lowest numeric value) becomes the STP root switch. If all switches have the same priority, the switch with the lowest MAC address will then become the root switch. The allowed range is 0 to 61440. The lower the numeric value you assign, the higher the priority for this bridge. Bridge Priority determines the root bridge, which in turn determines Hello Time, Max Age and Forwarding Delay.
Hello Time	This is the time interval in seconds between BPDU (Bridge Protocol Data Units) configuration message generations by the root switch. The allowed range is 1 to 10 seconds.
MAX Age	This is the maximum time (in seconds) a switch can wait without receiving a BPDU before attempting to reconfigure. All switch ports (except for designated ports) should receive BPDUs at regular intervals. Any port that ages out STP information (provided in the last BPDU) becomes the designated port for the attached LAN. If it is a root port, a new root port is selected from among the switch ports attached to the network. The allowed range is 6 to 40 seconds.
Forwarding Delay	This is the maximum time (in seconds) a switch will wait before changing states. This delay is required because every switch must receive information about topology changes before it starts to forward frames. In addition, each port needs time to listen for conflicting information that would make it return to a blocking state; otherwise, temporary data loops might result. The allowed range is 4 to 30 seconds. As a general rule: 2 * (Forward Delay - 1) >= Max Age >= 2 * (Hello Time + 1)
Port	This field identifies the Ethernet port.
Active	Select this check box to activate STP on this port.
Priority	Configure the priority for each port here. Priority decides which port should be disabled when more than one port forms a loop in a switch. Ports with a higher priority numeric value are disabled first. The allowed range is between 0 and 255 and default value is 128.

Table 51 RSTP Config (continued)

LABEL	DESCRIPTION
Path Cost	Path cost is the cost of transmitting a frame on to a LAN through that port. It is assigned according to the speed of the bridge. The slower the media, the higher the cost.
Apply	Click **Apply** to save your changes to the IP DSLAM's volatile memory. The IP DSLAM loses these changes if it is turned off or loses power, so use the **Config Save** link on the navigation panel to save your changes to the non-volatile memory when you are done configuring.
Cancel	Click **Cancel** to begin configuring this screen afresh.

27

Port Authentication

This chapter describes the 802.1x authentication method and RADIUS server connection setup.

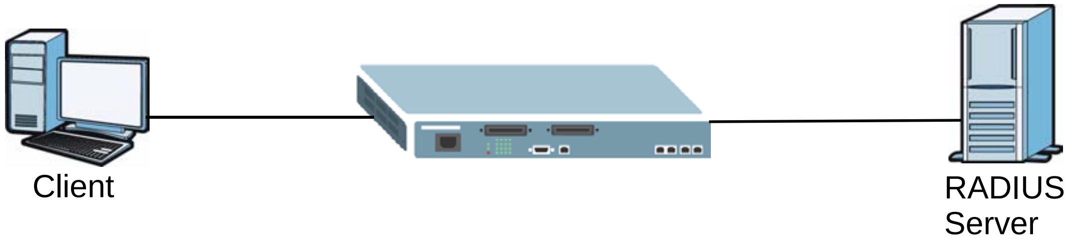
27.1 Introduction to Authentication

IEEE 802.1x is an extended authentication protocol[1] that allows support of RADIUS (Remote Authentication Dial In User Service, RFC 2138, 2139) for centralized user profile management on a network RADIUS server.

27.1.1 RADIUS

RADIUS (Remote Authentication Dial-In User Service) authentication is a popular protocol used to authenticate users by means of an external server instead of (or in addition to) an internal device user database that is limited to the memory capacity of the device. In essence, RADIUS authentication allows you to validate an unlimited number of users from a central location.

Figure 86 RADIUS Server



27.1.2 Introduction to Local User Database

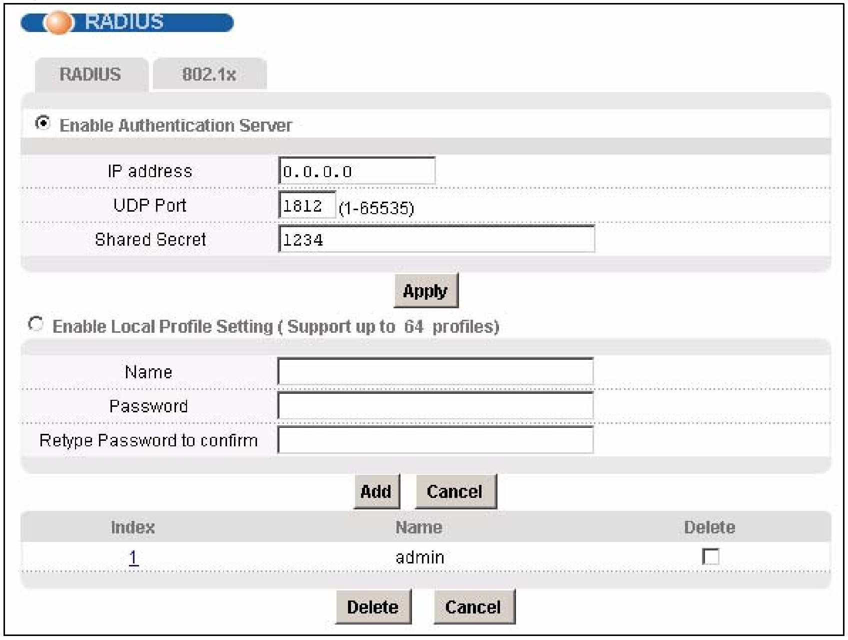
By storing user profiles locally on the IP DSLAM, your IP DSLAM is able to authenticate users without interacting

[1] At the time of writing, Windows XP of the Microsoft operating systems supports 802.1x. See the Microsoft web site for information on other Windows operating system support. For other operating systems, see its documentation. If your operating system does not support 802.1x, then you may need to install 802.1x client software.

27.2 RADIUS Screen

To open this screen, click **Advanced Application** > **Port Authentication**.

Figure 87 RADIUS



● Enable Authentication Server

IP address: 0.0.0.0

UDP Port: 1812 (1-65535)

Shared Secret: 1234

○ Enable Local Profile Setting (Support up to 64 profiles)

Name:

Password:

Retype Password to confirm:

Index	Name	Delete
1	admin	□

The following table describes the labels in this screen.

Table 52 RADIUS

LABEL	DESCRIPTION
Enable Authentication Server	Select this check box to have the IP DSLAM use an external RADIUS server to authenticate users.
IP Address	Enter the IP address of the external RADIUS server in dotted decimal notation.
UDP Port	The default port of the RADIUS server for authentication is **1812**. You need not change this value unless your network administrator instructs you to do so.
Shared Secret	Specify a password (up to 31 alphanumeric characters) as the key to be shared between the external RADIUS server and the switch. This key is not sent over the network. This key must be the same on the external RADIUS server and the switch.
Apply	Click **Apply** to save your changes to the IP DSLAM's volatile memory. The IP DSLAM loses these changes if it is turned off or loses power, so use the **Config Save** link on the navigation panel to save your changes to the non-volatile memory when you are done configuring.
Enable Local Authentication	Select this check box to have the IP DSLAM use its internal database of user names and passwords to authenticate users.
Name	Type the user name of the user profile.
Password	Type a password up to 31 characters long for this user profile.
Retype Password to confirm	Type the password again to make sure you have entered it properly.

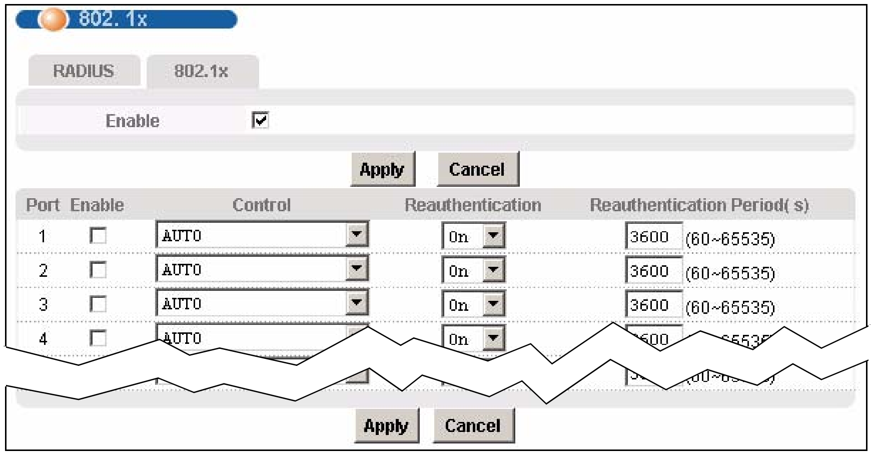
Table 52 RADIUS (continued)

LABEL	DESCRIPTION
Add	Click **Add** to save your changes to the IP DSLAM’s volatile memory. The IP DSLAM loses these changes if it is turned off or loses power, so use the **Config Save** link on the navigation panel to save your changes to the non-volatile memory when you are done configuring.
Cancel	Click **Cancel** to begin configuring this screen afresh.
	This table displays the configured user profiles.
Index	These are the numbers of the user profiles. Click this number to edit the user profile.
Name	This is the user name of the user profile.
Delete	Select a user profile’s **Delete** check box and click **Delete** to remove the user profile.
Cancel	Click **Cancel** to begin configuring this screen afresh and clear any selected **Delete** check boxes.

27.3 802.1x Screen

To open this screen, click **Advanced Application** > **Port Authentication** > **802.1x**.

Figure 88 802.1x



Enable ☑

Port	Enable	Control	Reauthentication	Reauthentication Period(s)
1	□	AUTO	On	3600 (60~65535)
2	□	AUTO	On	3600 (60~65535)
3	□	AUTO	On	3600 (60~65535)
4	□	AUTO	On	

The following table describes the labels in this screen.

Table 53 802.1x

LABEL	DESCRIPTION
Enable	Select this check box to turn on IEEE 802.1x authentication on the switch.
Apply	Click **Apply** to save your changes to the IP DSLAM’s volatile memory. The IP DSLAM loses these changes if it is turned off or loses power, so use the **Config Save** link on the navigation panel to save your changes to the non-volatile memory when you are done configuring.
Cancel	Click **Cancel** to begin configuring this screen afresh.
Port	This field displays a port number.
Enable	Select this check box to turn on IEEE 802.1x authentication on this port.

Table 53 802.1x (continued)

LABEL	DESCRIPTION
Control	Select **AUTO** to authenticate all subscribers before they can access the network through this port. Select **FORCE AUTHORIZED** to allow all connected users to access the network through this port without authentication. Select **FORCE UNAUTHORIZED** to deny all subscribers access to the network through this port.
Reauthentication	Specify whether a subscriber has to periodically re-enter his or her username and password to stay connected to the port (**On**) or not (**Off**).
Reauthentication Period(s)	Specify how often (in seconds) a client has to re-enter his or her username and password to stay connected to the port.
Apply	Click **Apply** to save your changes to the IP DSLAM's volatile memory. The IP DSLAM loses these changes if it is turned off or loses power, so use the **Config Save** link on the navigation panel to save your changes to the non-volatile memory when you are done configuring.
Cancel	Click **Cancel** to begin configuring this screen afresh.

28

Port Security

This chapter shows you how to set up port security.

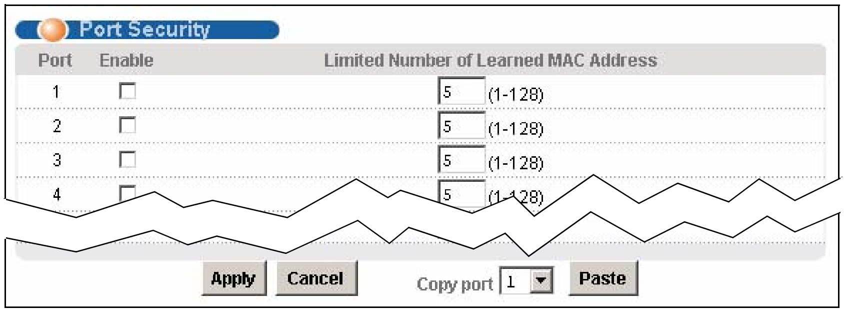
28.1 Port Security Overview

Port security allows you to restrict the number of MAC addresses that can be learned on a port. The IP DSLAM can learn up to 4K MAC addresses in total.

28.2 Port Security Screen

To open this screen, click **Advanced Application** > **Port Security**.

Figure 89   Port Security



Port Security

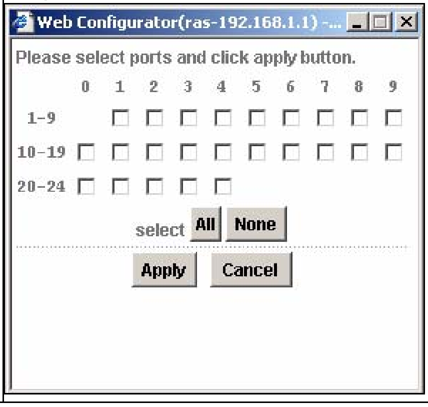
Port	Enable	Limited Number of Learned MAC Address
1	□	5 (1-128)
2	□	5 (1-128)
3	□	5 (1-128)
4	□	5 (1-128)

The following table describes the labels in this screen.

Table 54   Port Security

LABEL	DESCRIPTION
Port	This field displays a port number.
Enable	Select this check box to restrict the number of MAC addresses that can be learned on the port. Clear this check box to not limit the number of MAC addresses that can be learned on the port.
Limited Number of Learned MAC Address	Specify how many MAC addresses the IP DSLAM can learn on this port. The range is 1~128. Note: If you also use MAC filtering on a port, it is recommended that you set this limit to be equal to or greater than the number of MAC filter entries you configure.

Table 54 Port Security (continued)

LABEL	DESCRIPTION
Apply	Click **Apply** to save your changes to the IP DSLAM's volatile memory. The IP DSLAM loses these changes if it is turned off or loses power, so use the **Config Save** link on the navigation panel to save your changes to the non-volatile memory when you are done configuring.
Cancel	Click **Cancel** to begin configuring this screen afresh.
Copy port Paste	Do the following to copy settings from one port to another port or ports. 1. Select the number of the port from which you want to copy settings. 2. Click **Paste** and the following screen appears. 3. Select to which ports you want to copy the settings. Use **All** to select every port. Use **None** to clear all of the check boxes. 4. Click **Apply** to paste the settings. **Figure 90** Select Ports  Please select ports and click apply button. 0 1 2 3 4 5 6 7 8 9 1-9 □ □ □ □ □ □ □ □ □ 10-19 □ □ □ □ □ □ □ □ □ □ 20-24 □ □ □ □ □ Web Configurator(ras-192.168.1.1) -... select All None Apply Cancel

29

DHCP Relay

This chapter shows you how to set up DHCP relays for each VLAN.

29.1 DHCP Relay

DHCP (Dynamic Host Configuration Protocol, RFC 2131 and RFC 2132) allows individual clients to obtain TCP/IP configuration at start-up from a DHCP server. You can configure the IP DSLAM to relay DHCP requests to one or more DHCP servers and the server's responses back to the clients. You can specify default DHCP servers for all VLAN, and you can specify DHCP servers for each VLAN.

29.2 DHCP Relay Agent Information Option (Option 82)

The IP DSLAM can add information to DHCP requests that it relays to a DHCP server. This helps provide authentication about the source of the requests. You can also specify additional information for the IP DSLAM to add to the DHCP requests that it relays to the DHCP server. Please see RFC 3046 for more details.

The DHCP relay agent information feature adds an Agent Information field to the option 82 field of the DHCP headers of client TCP/IP configuration request frames that the IP DSLAM relays to a DHCP server. The IP DSLAM supports two formats for the DHCP relay agent information: Private and TR-101.

29.2.1 TR-101 Format

The Agent Information field that the IP DSLAM adds contains an "Agent Circuit-ID sub-option" that includes the system name or IP address, slot ID, port number, VPI, and VCI on which the TCP/IP configuration request was received.

The following figure shows the format of the TR-101 Agent Circuit ID sub-option. The 1 in the first field identifies this as an Agent Circuit ID sub-option. The next field specifies the length of the field. The hostname field displays the system name, if it has been configured, the extra information field (A) if the hostname was not configured, or the IP address in dotted decimal notation (w.x.y.z), if neither the system name nor the extra information field was been configured. In either case, the hostname is truncated to 23 characters, and trailing spaces are discarded. The hostname field is followed by a space, the string "atm", and another space. Then, a 1-byte Slot ID field specifies the ingress slot number (the IP DSLAM's slot ID is always 0), and a 1-byte Port No field specifies the ingress port number. Next, the VPI and VCI denote the virtual circuit that received the DHCP request message from the subscriber.

The slot ID, port number, VPI, VCI and MAC are separated from each other by a forward slash (/) colon (:) or period (.). An example is “SYSNAME atm 0/10:0.33”.

Table 55 DHCP Relay Agent Circuit ID Sub-option Format: TR-101 for VDSL

1	N	hostname / A / IP	“ eth “	Slot ID	/	Port No.

Table 56 DHCP Relay Agent Circuit ID Sub-option Format: TR-101 for ADSL

1	N	hostname / A / IP	“ atm “	Slot ID	/	Port No.	:	VPI	.	VCI

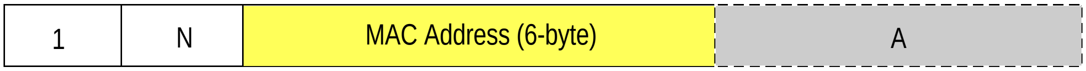
TR-101 uses the same remote ID sub-option format as the Private format.

29.2.2 Private Format

The DHCP relay agent information feature adds an Agent Information field to the option 82 field of the DHCP headers of DHCP request frames that the IP DSLAM relays to a DHCP server. The Agent Information field that the IP DSLAM adds contains an “Agent Circuit-ID sub-option” that includes the port number, VLAN ID and optional information about the port where the DHCP request was received.

The following figure shows the format of the Agent Circuit ID sub-option. The 1 in the first field identifies this as an Agent Circuit ID sub-option. The length N gives the total number of octets in the Agent Information Field. If the configuration request was received on an xDSL port, a 6-byte IP DSLAM's MAC address is added. The last field (A) can range from 0 to 24 bytes and is optional information (that you specify) about this relay agent.

Figure 91 DHCP Relay Agent Circuit ID Sub-option Format

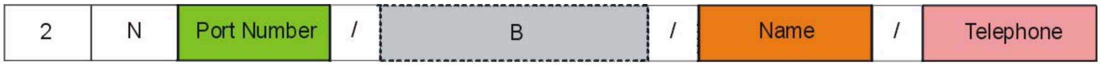


1	N	MAC Address (6-byte)	A

The Agent Information field that the IP DSLAM adds also contains an “Agent Remote-ID sub-option” of information that you specify.

The following figure shows the format of the Agent Remote ID sub-option. The 2 in the first field identifies this as an Agent Remote ID sub-option. The length N gives the total number of octets in the Agent Information Field. Then there is the number of the port (in plain text format) upon which the DHCP client request was received. The next field (B in the figure) is 0 to 23 bytes of optional information that you specify. This is followed by the name and telephone number configured for the xDSL port. The port number, optional information (B in the figure), xDSL name and xDSL telephone number fields are separated by forward slashes.

Figure 92 DHCP Relay Agent Remote ID Sub-option Format

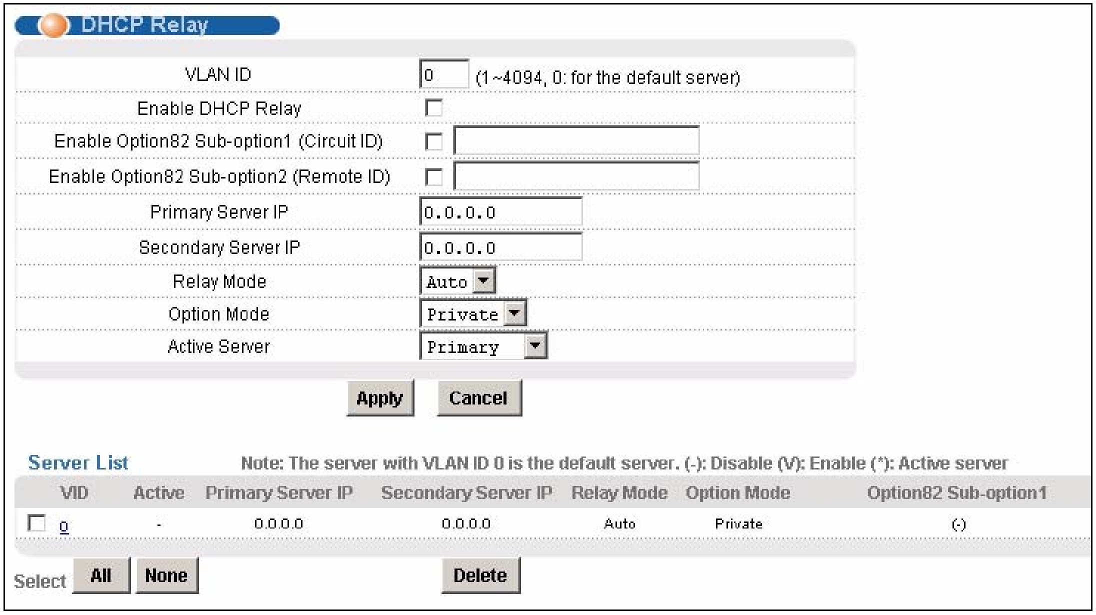


2	N	Port Number	/	B	/	Name	/	Telephone

29.3 DHCP Relay Screen

To open this screen, click **Advanced Application** > **DHCP Relay**.

Figure 93 DHCP Relay



VLAN ID	0 (1~4094, 0: for the default server)
Enable DHCP Relay	□
Enable Option82 Sub-option1 (Circuit ID)	□
Enable Option82 Sub-option2 (Remote ID)	□
Primary Server IP	0.0.0.0
Secondary Server IP	0.0.0.0
Relay Mode	Auto
Option Mode	Private
Active Server	Primary

Server List Note: The server with VLAN ID 0 is the default server. (-): Disable (V): Enable (*): Active server

	VID	Active	Primary Server IP	Secondary Server IP	Relay Mode	Option Mode	Option82 Sub-option1
□	0	-	0.0.0.0	0.0.0.0	Auto	Private	(-)

The following table describes the labels in this screen.

Table 57 DHCP Relay

LABEL	DESCRIPTION
VLAN ID	Enter the ID of the VLAN served by the specified DHCP relay(s). Enter 0 to set up the default DHCP relay(s).
Enable DHCP Relay:	Select this to have the IP DSLAM relay DHCP requests in the selected VLAN to a DHCP server and the server’s responses back to the clients.
Enable Option82 Sub-option1 (Circuit ID)	Select this to have the IP DSLAM add the originating port numbers to DHCP requests in the selected VLAN regardless of whether the DHCP relay is on or off. In the field next to the check box, you can also specify up to 23 ASCII characters of additional information for the IP DSLAM to add to the DHCP requests that it relays to a DHCP server. Examples of information you could add would be the chassis number of the IP DSLAM or the ISP’s name.
Enable Option82 Sub-option2 (Remote ID)	Enable DHCP relay info to have the IP DSLAM add the sub-option 2 (Remote ID) to DHCP requests in the selected VLAN regardless of whether the DHCP relay is on or off. In the field next to the check box, you can also specify up to 23 ASCII characters of additional information for the IP DSLAM to add to the DHCP requests that it relays to a DHCP server.
Primary Server IP	Enter the IP address of one DHCP server to which the switch should relay DHCP requests for the selected VLAN.
Secondary Server IP	Enter the IP address of a second DHCP server to which the switch should relay DHCP requests for the selected VLAN. Enter 0.0.0.0 if there is only one DHCP relay for the selected VLAN.
Relay Mode	Specify how the IP DSLAM relays DHCP requests for the selected VLAN. **Auto** - The IP DSLAM routes DHCP requests to the active server for the VLAN. **Both** - The IP DSLAM routes DHCP requests to the primary and secondary server for the VLAN, regardless of which one is active.
Option Mode	Specify the type of format (**Private or TR101**) the IP DSLAM uses when editing DHCP relay agent information to DHCP requests. See Section 29.2 on page 173.
Active Server	This field has no effect if the **Relay Mode** is **Both**. If the **Relay Mode** is **Auto**, select which DHCP server (the primary one or the secondary one) to which the IP DSLAM should relay DHCP requests for the selected VLAN.

Table 57 DHCP Relay (continued)

LABEL	DESCRIPTION
Apply	Click **Apply** to save your changes to the IP DSLAM's volatile memory. The IP DSLAM loses these changes if it is turned off or loses power, so use the **Config Save** link on the navigation panel to save your changes to the non-volatile memory when you are done configuring.
Cancel	Click **Cancel** to begin configuring this screen afresh.
Server List	This section lists the current DHCP relay settings for each VLAN. An asterisk in parentheses (*) indicates which DHCP server is active for each VLAN.
VID	This field displays the ID of the VLAN served by the specified DHCP relay(s).
Active	This field displays whether or not the IP DSLAM relays DHCP requests in the selected VLAN to a DHCP server and the server's responses back to the clients.
Primary Server IP	This field displays the IP address of one DHCP server to which the switch should relay DHCP requests. If this is the active server for the selected VLAN, it is marked with an asterisk (*).
Secondary Server IP	This field displays the IP address of a second DHCP server to which the switch should relay DHCP requests. This field is 0.0.0.0 if the primary server is the only DHCP relay. If this is the active server for the selected VLAN, it is marked with an asterisk (*).
Relay Mode	This field displays how the IP DSLAM relays DHCP requests for the selected VLAN. **Auto** - The IP DSLAM routes DHCP requests to the active server for the VLAN. **Both** - The IP DSLAM routes DHCP requests to the primary and secondary server for the VLAN, regardless of which one is active.
Option Mode	This field displays which format (**Private** or **TR101**) the IP DSLAM uses to add DHCP relay agent information to DHCP requests.
Option82 Sub-option1	This field displays whether or not the IP DSLAM adds the originating port numbers (and any additional information) to DHCP requests in the selected VLAN.
Option82 Sub-option2	This field displays whether or not the IP DSLAM adds the sub-option 2 (and any additional information) to DHCP requests in the selected VLAN.
Delete	Select the check box next to the VLAN ID, and click **Delete** to remove the entry.
Select All	Click this to select all entries in the **Server List**.
Select None	Click this to un-select all entries in the **Server List**.

30

DHCP Snoop

This chapter shows you how to set up DHCP snooping settings on the subscriber ports.

30.1 DHCP Snoop Overview

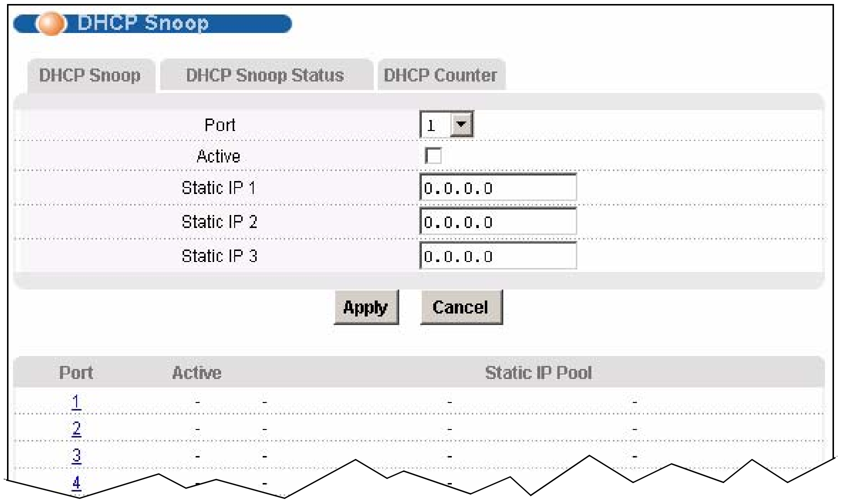
DHCP snooping prevents clients from assigning their own IP addresses. The IP DSLAM can store every (ADSL port, MAC address, IP address) tuple offered by the DHCP server. Then, it only forwards packets from clients whose MAC address and IP address are recorded. Packets from unknown IP addresses are dropped.

In some cases, you might want to allow packets from an IP address not offered by the DHCP server. This might apply, for example, when a device uses a static IP address. In this case, you can specify the IP address whose packets are allowed, and the IP DSLAM forwards these packets as well.

30.2 DHCP Snoop Screen

Use this screen to activate or deactivate DHCP snooping on each port. To open this screen, click **Advanced Application** > **DHCP Snoop**.

Figure 94 DHCP Snoop



Port	1
Active	□
Static IP 1	0.0.0.0
Static IP 2	0.0.0.0
Static IP 3	0.0.0.0

Port	Active	Static IP Pool		
1	-	-	-	-
2	-	-	-	-
3	-	-	-	-
4	-	-	-	

The following table describes the labels in this screen.

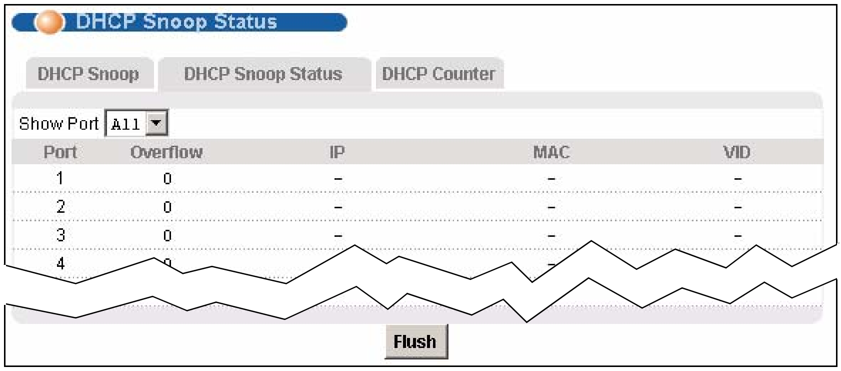
Table 58 DHCP Snoop

LABEL	DESCRIPTION
Port	This field displays each xDSL port number. Click a port to bring the setting on the first section of the screen.
Active	Specify whether DHCP snooping is active (“V”) or inactive (“-”) on this port.
Static IP 1~3	These fields are only effective when DHCP snooping is active. Enter up to three IP addresses for which the IP DSLAM should forward packets, even if the IP address is not assigned by the DHCP server. The IP DSLAM drops packets from other unknown IP addresses on this port. To delete an existing IP address, enter **0.0.0.0**.
Apply	Click **Apply** to save your changes to the IP DSLAM’s volatile memory. The IP DSLAM loses these changes if it is turned off or loses power, so use the **Config Save** link on the navigation panel to save your changes to the non-volatile memory when you are done configuring.
Cancel	Click **Cancel** to begin configuring this screen afresh.
Port	This field displays each xDSL port number. Click a port number to edit it in the section above.
Active	This field displays whether DHCP snooping is active (“V”) or inactive (“-”) on this port.
Static IP Pool	These fields display IP addresses for which the IP DSLAM should forward packets, even if the IP address is not assigned by the DHCP server. “-“ displays for a blank value.

30.3 DHCP Snoop Status Screen

Use this screen to look at or to clear the DHCP snooping table on each port. To open this screen, click **Advanced Application** > **DHCP Snoop** > **DHCP Snoop Status**.

Figure 95 DHCP Snoop Status



Show Port All

Port	Overflow	IP	MAC	VID
1	0	–	–	–
2	0	–	–	–
3	0	–	–	–
4	0		–	

The following table describes the labels in this screen.

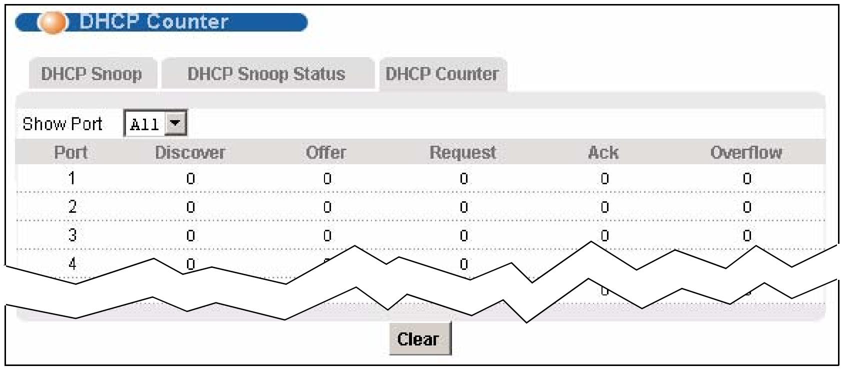
Table 59 DHCP Snoop Status

LABEL	DESCRIPTION
Show Port	Select a port for which you wish to view information.
Port	This field displays the selected xDSL port number(s).
Overflow	There is a limit to the number of IP addresses the DHCP server can assign at one time to each port. This field displays the number of requests from DHCP clients above this limit. Overflow requests are dropped by the IP DSLAM.
IP	This field displays the IP address assigned to a client on this port.
MAC	This field displays the MAC address of a client on this port to which the DHCP server assigned an IP address.
VID	This field displays the VLAN ID, if any, on the DHCP Request packet.
Flush	Click **Flush** to remove all of the entries from the DHCP snooping table for the selected port(s).

30.4 DHCP Counter Screen

Use this screen to look at a summary of the DHCP packets on each port. To open this screen, click **Advanced Application** > **DHCP Snoop** > **DHCP Counter**.

Figure 96 DHCP Counter



Port	Discover	Offer	Request	Ack	Overflow
1	0	0	0	0	0
2	0	0	0	0	0
3	0	0	0	0	0
4	0		0		

The following table describes the labels in this screen.

Table 60 DHCP Counter

LABEL	DESCRIPTION
Show Port	Select a port for which you wish to view information.
Port	This field displays the selected xDSL port number(s).
Discover	This field displays the number of DHCP Discover packets on this port.
Offer	This field displays the number of DHCP Offer packets on this port.
Request	This field displays the number of DHCP Request packets on this port.
Ack	This field displays the number of DHCP Acknowledge packets on this port.

Table 60 DHCP Counter (continued)

LABEL	DESCRIPTION
Overflow	There is a limit to the number of IP addresses the DHCP server can assign at one time to each port. This field displays the number of requests from DHCP clients above this limit. Overflow requests are dropped by the IP DSLAM.
Clear	Click **Clear** to delete the information the IP DSLAM has learned about DHCP packets. This resets every counter in this screen.

31

2684 Routed Mode

This chapter shows you how to set up 2684 routed mode service.

31.1 2684 Routed Mode

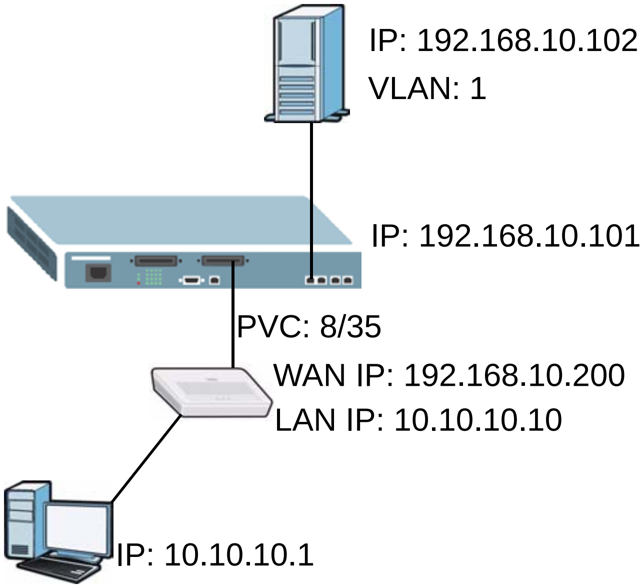
Use the 2684 (formerly 1483) routed mode to have the IP DSLAM add MAC address headers to 2684 routed mode traffic from a PVC that connects to a subscriber device that uses 2684 routed mode. You also specify the gateway to which the IP DSLAM sends the traffic and the VLAN ID tag to add. See RFC-2684 for details on routed mode traffic carried over AAL type 5 over ATM.

- Use the 2684 Routed PVC Screen to configure PVCs for 2684 routed mode traffic.
- Use the 2684 Routed Domain Screen to configure domains for 2684 routed mode traffic. The domain is the range of IP addresses behind the subscriber’s device (the CPE or Customer Premises Equipment). This includes the CPE device’s LAN IP addresses and the IP addresses of the LAN computers.
- Use the RPVC Arp Proxy Screen to view the Address Resolution Protocol table of IP addresses of CPE devices using 2684 routed mode and configure how long the device is to store them.
- Use the 2684 Routed Gateway Screen to configure gateway settings.
- For upstream traffic: Since the subscriber's device will not send out a MAC address, after the IP DSLAM reassembles the Ethernet packets from the AAL5 ATM cells, the IP DSLAM will append the routed mode gateway's MAC address and the IP DSLAM's MAC address as the destination/source MAC address.
- For downstream traffic: When the IP DSLAM sees the destination IP address is specified in the RPVC (or RPVC domain), the IP DSLAM will strip out the MAC header and send them to the corresponding RPVC.

31.1.1 2684 Routed Mode Example

The following figure shows an example 2684 routed mode set up. The gateway server uses IP address 192.168.10.102 and is in VLAN 1. The IP DSLAM uses IP address 192.168.10.101. The subscriber’s device (the CPE) is connected to DSL port 1 on the IP DSLAM and the 2684 routed mode traffic is to use the PVC identified by VPI 8 and VCI 35. The CPE device’s WAN IP address is 192.168.10.200. The routed domain is the LAN IP addresses behind the CPE device. The CPE device’s LAN IP address is 10.10.10.10 and the LAN computer’s IP address is 10.10.10.1. This includes the CPE device’s LAN IP addresses and the IP addresses of the LAN computers.

Figure 97 2684 Routed Mode Example



Note the following.

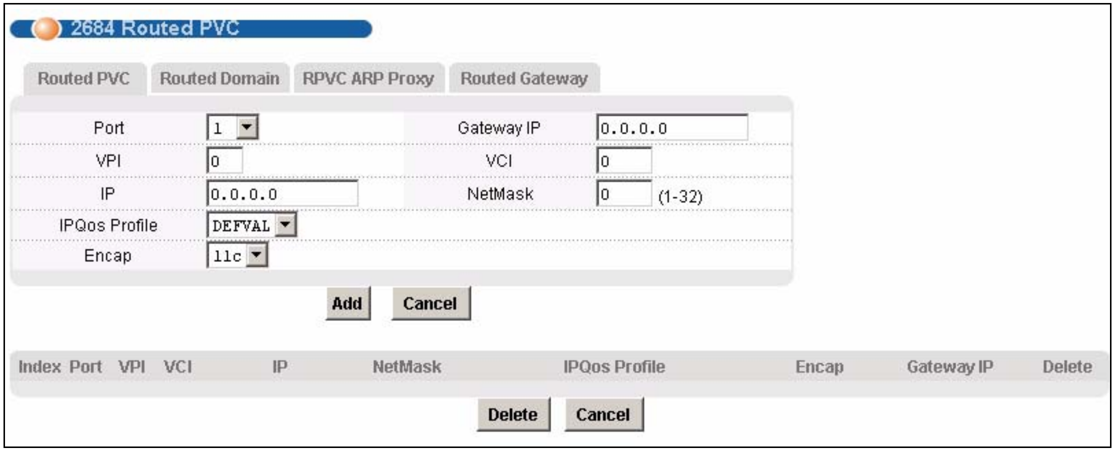
- The CPE device’s WAN IP (192.168.10.200 in this example) must be in the same subnet as the gateway’s IP address (192.168.10.102 in this example).
- The IP DSLAM's management IP address can be any IP address, it doesn't have any relationship to the WAN IP address or routed gateway IP address.
- The IP DSLAM’s management IP address should not be in the same subnet as the one defined by the WAN IP address and netmask of the subscriber’s device. It is suggested that you set the netmask of the subscriber’s WAN IP address to 32 to avoid this problem.
- The IP DSLAM's management IP address should not be in the same subnet range of any RPVC and RPVC domain. It will make the IP DSLAM confused if the IP DSLAM0 receives a packet with this IP as destination IP.
- The IP DSLAM’s management IP address also should not be in the same subnet as the one defined by the LAN IP address and netmask of the subscriber’s device. Make sure you assign the IP addresses properly.
- In general deployment, the computer must set the CPE device’s LAN IP address (10.10.10.10 in this example) as its default gateway.
- The subnet range of any RPVC and RPVC domain must be unique.

31.2 2684 Routed PVC Screen

Use this screen to configure PVCs for 2684 routed mode traffic.

To open this screen, click **Advanced Application** > **2684 Routed Mode**.

Figure 98 2684 Routed PVC



Port	1	Gateway IP	0.0.0.0
VPI	0	VCI	0
IP	0.0.0.0	NetMask	0 (1-32)
IPQos Profile	DEFVAL		
Encap	llc		

Index	Port	VPI	VCI	IP	NetMask	IPQos Profile	Encap	Gateway IP	Delete

The following table describes the labels in this screen.

Table 61 2684 Routed PVC

LABEL	DESCRIPTION
Port	Use this drop-down list box to select a port for which you wish to configure settings.
Gateway IP	Enter the IP address of the gateway to which you want to send the traffic that the system receives from this PVC. Enter the IP address in dotted decimal notation.
VPI	Type the Virtual Path Identifier for this routed PVC.
VCI	Type the Virtual Circuit Identifier for this routed PVC.
IP	Enter the subscriber’s CPE WAN IP address in dotted decimal notation.
NetMask	The bit number of the subnet mask of the subscriber’s WAN IP address. To find the bit number, convert the subnet mask to binary and add all of the 1’s together. Take “255.255.255.0” for example. 255 converts to eight 1’s in binary. There are three 255’s, so add three eights together and you get the bit number (24). Make sure that the routed PVC’s subnet does not include the IP DSLAM’s IP address.
IPQos Profile	Select an IPQoS profile to classify and prioritize application traffic flowing through this PVC. Use the **Basic Settings** > **xDSL Profiles Setup** > **IPQos Profile** screen to configure IPQoS profiles. See Section 17.2 on page 119.
Encap	Select an encapsulation method (**llc** or **vc**) for this PVC.
Add	Click **Add** to save your changes to the IP DSLAM’s volatile memory. The IP DSLAM loses these changes if it is turned off or loses power, so use the **Config Save** link on the navigation panel to save your changes to the non-volatile memory when you are done configuring.
Cancel	Click **Cancel** to start configuring the screen again.
Index	This field displays the number of the routed PVC.
Port	This field displays the number of the xDSL port on which the routed PVC is configured.
VPI	This field displays the Virtual Path Identifier (VPI) The VPI and VCI identify a channel on this port.
VCI	This field displays the Virtual Circuit Identifier (VCI). The VPI and VCI identify a channel on this port.
IP	This field displays the subscriber’s IP address.

Table 61 2684 Routed PVC (continued)

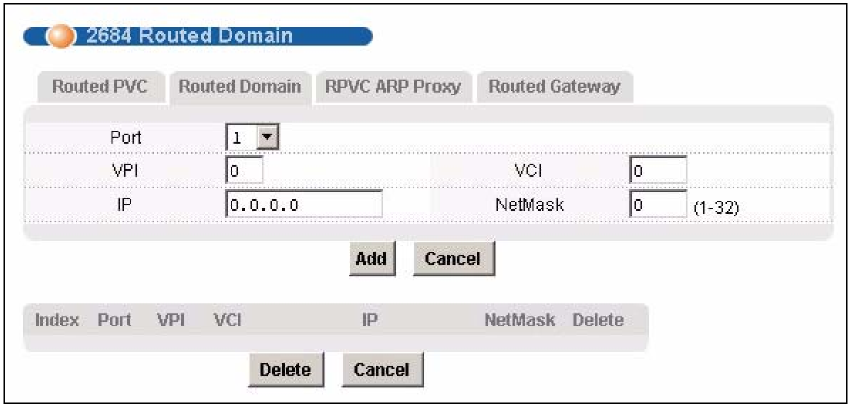
LABEL	DESCRIPTION
NetMask	This field displays the bit number of the subnet mask of the subscriber's IP address.
IPQos Profile	This field displays the IPQoS profile configured for this PVC.
Encap	This field displays the encapsulation method (**llc** or **vc**) configured for this PVC.
Gateway IP	This field displays the IP address of the gateway to which you want to send the traffic that the system receives from this PVC.
Delete	Select an entry's **Delete** check box and click **Delete** to remove the entry. Clicking **Delete** saves your changes to the IP DSLAM's volatile memory. The IP DSLAM loses these changes if it is turned off or loses power, so use the **Config Save** link on the navigation panel to save your changes to the non-volatile memory when you are done configuring.
Cancel	Click **Cancel** to start configuring the screen again.

31.3 2684 Routed Domain Screen

Use this screen to configure domains for 2684 routed mode traffic. The domain is the range of IP addresses behind the subscriber's device (the CPE). This includes the CPE device's LAN IP addresses and the IP addresses of the LAN computers.

To open this screen, click **Advanced Application** > **2684 Routed Mode** > **Routed Domain**.

Figure 99 2684 Routed Domain



Port	1		
VPI	0	VCI	0
IP	0.0.0.0	NetMask	0 (1-32)

The following table describes the labels in this screen.

Table 62 2684 Routed Domain

LABEL	DESCRIPTION
Port	Use this drop-down list box to select a port for which you wish to configure settings.
VPI	Type the Virtual Path Identifier for this routed PVC.
VCI	Type the Virtual Circuit Identifier for this routed PVC.
IP	Enter the subscriber's CPE LAN IP address in dotted decimal notation.
NetMask	The bit number of the subnet mask of the subscriber's IP address. To find the bit number, convert the subnet mask to binary and add all of the 1's together. Take "255.255.255.0" for example. 255 converts to eight 1's in binary. There are three 255's, so add three eights together and you get the bit number (24).

Table 62 2684 Routed Domain (continued)

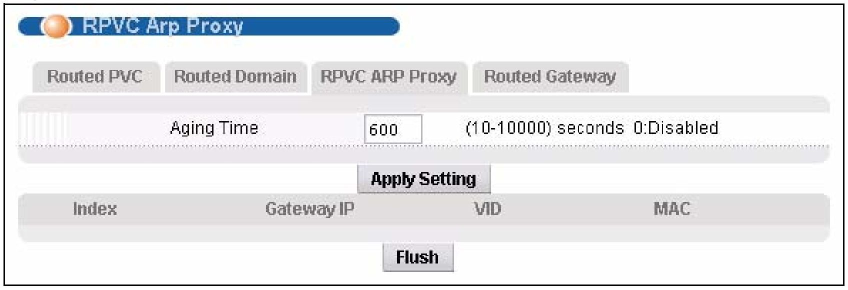
LABEL	DESCRIPTION
Add	Click **Add** to save your changes to the IP DSLAM's volatile memory. The IP DSLAM loses these changes if it is turned off or loses power, so use the **Config Save** link on the navigation panel to save your changes to the non-volatile memory when you are done configuring.
Cancel	Click **Cancel** to start configuring the screen again.
Index	This field displays the number of the routed PVC.
Port	This field displays the number of the xDSL port on which the routed PVC is configured.
VPI	This field displays the Virtual Path Identifier (VPI) The VPI and VCI identify a channel on this port.
VCI	This field displays the Virtual Circuit Identifier (VCI). The VPI and VCI identify a channel on this port.
IP	This field displays the subscriber's IP address.
NetMask	This field displays the bit number of the subnet mask of the subscriber's LAN IP address.
Delete	Select an entry's **Delete** check box and click **Delete** to remove the entry. Clicking **Delete** saves your changes to the IP DSLAM's volatile memory. The IP DSLAM loses these changes if it is turned off or loses power, so use the **Config Save** link on the navigation panel to save your changes to the non-volatile memory when you are done configuring.
Cancel	Click **Cancel** to start configuring the screen again.

31.4 RPVC Arp Proxy Screen

Use this screen to view the Address Resolution Protocol table of IP addresses of CPE devices using 2684 routed mode and configure how long the device is to store them.

To open this screen, click **Advanced Application** > **2684 Routed Mode** > **RPVC ARP Proxy**.

Figure 100 RPVC Arp Proxy



Aging Time 600 (10-10000) seconds 0:Disabled

The following table describes the labels in this screen.

Table 63 RPVC Arp Proxy

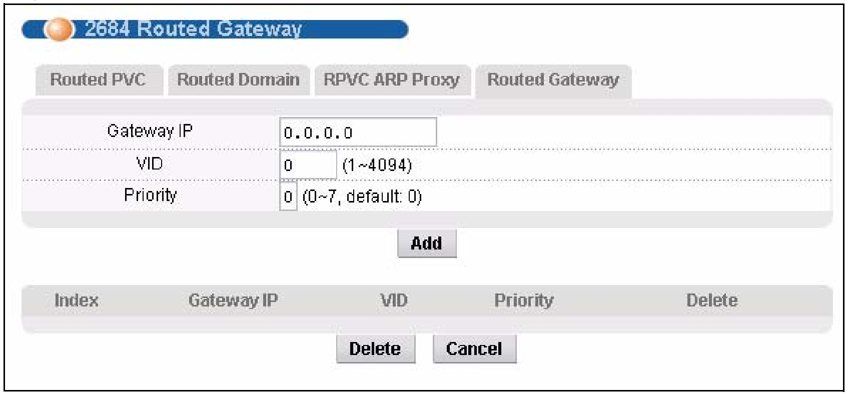
LABEL	DESCRIPTION
Aging Time	Enter a number of seconds (10~10000) to set how long the device keeps the Address Resolution Protocol table's entries of IP addresses of CPE devices using 2684 routed mode. Enter 0 to disable the aging time.
Apply Setting	Click **Apply Setting** to save your changes to the IP DSLAM's volatile memory. The IP DSLAM loses these changes if it is turned off or loses power, so use the **Config Save** link on the navigation panel to save your changes to the non-volatile memory when you are done configuring.
Index	This field displays the number of the IP address entry.
Gateway IP	This field displays the IP address of the gateway to which the device sends the traffic that it receives from this entry's IP address.
VID	This field displays the VLAN Identifier that the device adds to Ethernet frames that it sends to this gateway.
MAC	This field displays the subscriber's MAC (Media Access Control) address.
Flush	Click **Flush** to remove all of the entries from the ARP table.

31.5 2684 Routed Gateway Screen

Use this screen to configure gateway settings.

To open this screen, click **Advanced Application** > **2684 Routed Mode** > **Routed Gateway**.

Figure 101 2684 Routed Gateway



Gateway IP	0.0.0.0
VID	0 (1~4094)
Priority	0 (0~7, default: 0)

Index	Gateway IP	VID	Priority	Delete

The following table describes the labels in this screen.

Table 64 2684 Routed Gateway

LABEL	DESCRIPTION
Gateway IP	Enter the IP address of the gateway to which you want to send the traffic that the system receives from this PVC. Enter the IP address in dotted decimal notation.
VID	Specify a VLAN Identifier to add to Ethernet frames that the system routes to this gateway.
Priority	Select the IEEE 802.1p priority (0~7) to add to the traffic that you send to this gateway.

Table 64 2684 Routed Gateway (continued)

LABEL	DESCRIPTION
Add	Click **Add** to save your changes to the IP DSLAM’s volatile memory. The IP DSLAM loses these changes if it is turned off or loses power, so use the **Config Save** link on the navigation panel to save your changes to the non-volatile memory when you are done configuring.
Index	This field displays the number of the gateway entry.
Gateway IP	This field displays the IP address of the gateway.
VID	This field displays the VLAN Identifier that the system adds to Ethernet frames that it sends to this gateway.
Priority	This field displays the IEEE 802.1p priority (0~7) that is added to traffic sent to this gateway.
Delete	Select an entry’s **Delete** check box and click **Delete** to remove the entry. Clicking **Delete** saves your changes to the IP DSLAM’s volatile memory. The IP DSLAM loses these changes if it is turned off or loses power, so use the **Config Save** link on the navigation panel to save your changes to the non-volatile memory when you are done configuring.
Cancel	Click **Cancel** to start configuring the screen again.

32

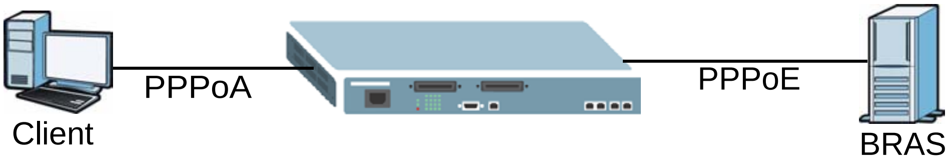
PPPoA to PPPoE

This chapter shows you how to set up the IP DSLAM to convert PPPoA frames to PPPoE traffic and vice versa.

32.1 PPPoA to PPPoE Overview

Before migrating to an Ethernet infrastructure, a broadband network might consist of PPPoA connections between the CPE devices and the DSLAM and PPPoE connections from the DSLAM to the Broadband Remote Access Server (BRAS). The following figure shows a network example.

Figure 102 Mixed PPPoA-to-PPPoE Broadband Network Example



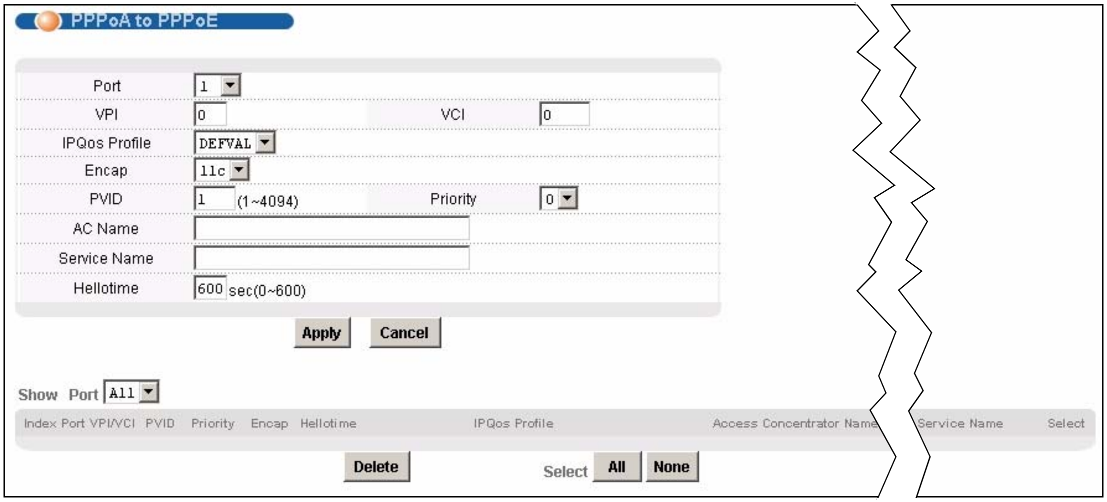
In order to allow communication between the end points (the CPE devices and the BRAS), you need to configure the DSLAM (the IP DSLAM) to translate PPPoA frames to PPPoE packets and vise versa.

When PPPoA packets are received from the CPE, the ATM headers are removed and the IP DSLAM adds PPPoE and Ethernet headers before sending the packets to the BRAS. When the IP DSLAM receives PPPoE packets from the BRAS, PPPoE and Ethernet headers are stripped and necessary PVC information (such as encapsulation type) is added before forwarding to the designated CPE.

32.2 PPPoA to PPPoE Screen

Use this screen to set up PPPoA to PPPoE conversions on each port. This conversion is set up by creating a PAE PVC. See Chapter 16 on page 99 for background information about creating PVCs. To open this screen, click **Advanced Application** > **PPPoA to PPPoE**.

Figure 103 PPPoA to PPPoE



PPPoA to PPPoE

Port	1		
VPI	0	VCI	0
IPQos Profile	DEFVAL		
Encap	llc		
PVID	1 (1~4094)	Priority	0
AC Name			
Service Name			
Hellotime	600 sec(0~600)		

Show Port All

Index	Port	VPI/VCI	PVID	Priority	Encap	Hellotime	IPQos Profile	Access Concentrator Name	Service Name	Select

The following table describes the labels in this screen.

Table 65 PPPoA to PPPoE

LABEL	DESCRIPTION
Port	Use this drop-down list box to select a port for which you wish to set up PPPoA to PPPoE conversions. This field is read-only once you click on a port number below.
VPI	Type the Virtual Path Identifier for a channel on this port.
VCI	Type the Virtual Circuit Identifier for a channel on this port.
IPQos Profile	Select an IPQoS profile to classify and prioritize application traffic flowing through this PVC. Use the **Basic Setting** > **xDSL Profiles Setup** > **IPQos Profile** screen to configure IPQoS profiles. See Section 17.2 on page 119.
Encap	Select an encapsulation method (**llc** or **vc**) for this PVC.
PVID	Type a PVID (Port VLAN ID) to assign to untagged frames received on this channel. Note: Make sure the VID is not already used for multicast VLAN or TLS PVC.
Priority	Use the drop-down list box to select the priority value (0 to 7) to add to incoming frames without a (IEEE 802.1p) priority tag.
AC Name	This field is optional. Specify the hostname of a remote access concentrator if there are two access concentrators (or BRAS) on the network or if you want to allow PAE translation to the specified access concentrator. In this case, the IP DSLAM checks the AC name field in the BRAS's reply PDU. If there is a mismatch, the IP DSLAM drops this PDU. (This is not recorded as an **PPPoE AC System Error** in the **PPPoA to PPPoE Status** screen, however.)
Service Name	This field is optional. Specify the name of the service that uses this PVC. This must be a service name that you configure on the remote access concentrator.
Hello Time	Specify the timeout, in seconds, for the PPPoE session. Enter 0 if there is no timeout.

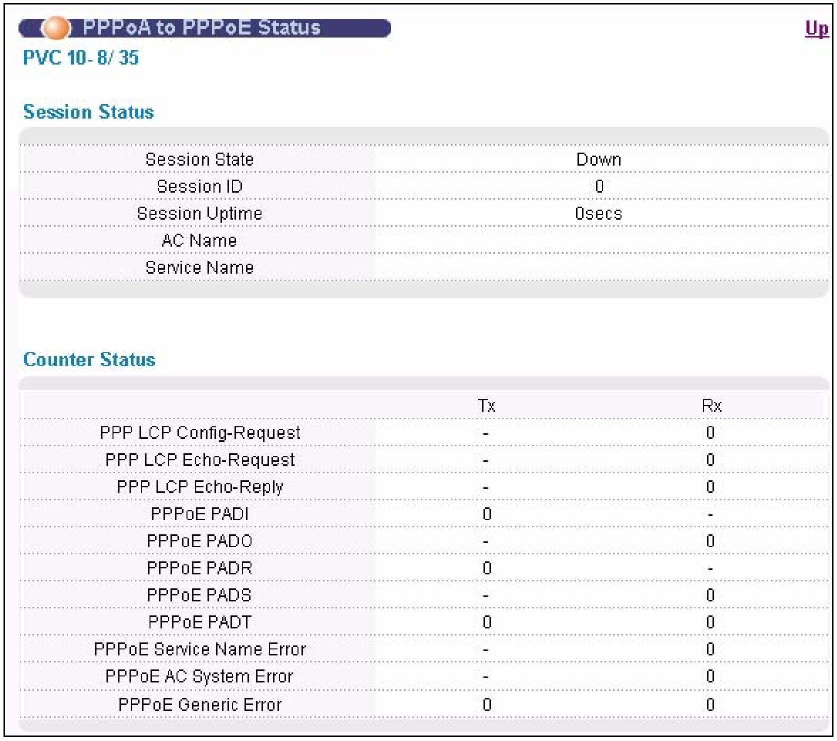
Table 65 PPPoA to PPPoE (continued)

LABEL	DESCRIPTION
Apply	Click this to add or save channel settings on the selected port. This saves your changes to the IP DSLAM's volatile memory. The IP DSLAM loses these changes if it is turned off or loses power, so use the **Config Save** link on the navigation panel to save your changes to the non-volatile memory when you are done configuring.
Cancel	Click **Cancel** to start configuring the screen again.
Show Port	Select which xDSL port(s) for which to display PPPoA to PPPoE conversion settings.
Index	This field displays the number of the PVC. Click a PVC's index number to open the screen where you can look at the current status of this PPPoA-to-PPPoE conversion. (See Section 32.3 on page 191.) Note: At the time of writing, you cannot edit the VPI and VCI. If you want to change them, add a new PVC with the desired settings. Then, delete any unwanted PVCs.
Port	This field displays the number of the xDSL port on which the PVC is configured.
VPI/VCI	This field displays the Virtual Path Identifier (VPI) and Virtual Circuit Identifier (VCI). The VPI and VCI identify a channel on this port.
PVID	This is the PVID (Port VLAN ID) assigned to untagged frames or priority frames (0 VID) received on this channel.
Priority	This is the priority value (0 to 7) added to incoming frames without a (IEEE 802.1p) priority tag.
Encap	This field displays the encapsulation method (**llc** or **vc**) applied on the PPPoA-to-PPPoE conversion.
Hello Time	This field displays the timeout for the PPPoE session, in seconds.
IPQos Profile	This field display the IPQoS profile applied on the PPPoA-to-PPPoE conversion.
Access Concentrator Name	This field displays the name of the specified remote access concentrator, if any.
Service Name	This field displays the name of the service that uses this PVC on the remote access concentrator.
Select Delete	Select the check box in the **Select** column for an entry, and click **Delete** to remove the entry.
Select All	Click this to select all entries in the table.
Select None	Click this to un-select all entries in the table.

32.3 PPPoA to PPPoE Status Screen

Use this screen to look at the current status of each PPPoA to PPPoE conversion. To open this screen, click **Advanced Application** > **PPPoA to PPPoE**, and then click an index number.

Figure 104 PPPoA to PPPoE Status



PVC 10- 8/ 35

Session Status

Session State	Down
Session ID	0
Session Uptime	0secs
AC Name	
Service Name	

Counter Status

	Tx	Rx
PPP LCP Config-Request	-	0
PPP LCP Echo-Request	-	0
PPP LCP Echo-Reply	-	0
PPPoE PADI	0	-
PPPoE PADO	-	0
PPPoE PADR	0	-
PPPoE PADS	-	0
PPPoE PADT	0	0
PPPoE Service Name Error	-	0
PPPoE AC System Error	-	0
PPPoE Generic Error	0	0

The following table describes the labels in this screen.

Table 66 PPPoA to PPPoE Status

LABEL	DESCRIPTION
PVC	This field displays the port number, VPI, and VCI of the PVC.
Session Status	
Session State	This field displays whether or not the current session is **Up** or **Down**.
Session ID	This field displays the ID of the current session. It displays **0** if there is no current session.
Session Uptime	This field displays how long the current session has been up.
AC Name	This field displays the hostname of the remote access concentrator if there are two access concentrators (or BRAS) on the network or if you want to allow PAE translation to the specified access concentrator.
Service Name	This field specifies the name of the service that uses this PVC.
Counter Status	
Tx/Rx	The values in these columns are for packets transmitted (`tx`) or received (`rx`) by the IP DSLAM.
PPP LCP Config-Request	This field displays the number of config-request PDUs received by the IP DSLAM from the CPE (client) device.
PPP LCP Echo-Request	This field displays the number of echo-request PDUs received by the IP DSLAM from the CPE (client) device.
PPP LCP Echo-Reply	This field displays the number of echo-reply PDUs received by the IP DSLAM from the CPE (client) device.
PPPoE PADI	This field displays the number of padi PDUs sent by the IP DSLAM to the BRAS.

Table 66 PPPoA to PPPoE Status (continued)

LABEL	DESCRIPTION
PPPoE PADO	This field displays the number of pado PDUs sent by the BRAS to the IP DSLAM.
PPPoE PADR	This field displays the number of padr PDUs sent by the IP DSLAM to the BRAS.
PPPoE PADS	This field displays the number of pads PDUs sent by the BRAS to the IP DSLAM.
PPPoE PADT	This field displays the number of padt PDUs sent and received by the IP DSLAM.
PPPoE Service Name Error	This field displays the number of service name errors; for example, the IP DSLAM’s specified service is different than the BRAS’s setting.
PPPoE AC System Error	This field displays the number of times the access concentrator experienced an error while performing the Host request; for example, when resources are exhausted in the access concentrator. This value does not include the number of times the IP DSLAM checks the AC name field in the BRAS's reply PDU and finds a mismatch, however.
PPPoE Generic Error	This field displays the number of other types of errors that occur in the PPPoE session between the IP DSLAM and the BRAS.

33

DSCP

This chapter shows you how to set up DSCP on each port and how to convert DSCP values to IEEE 802.1p values.

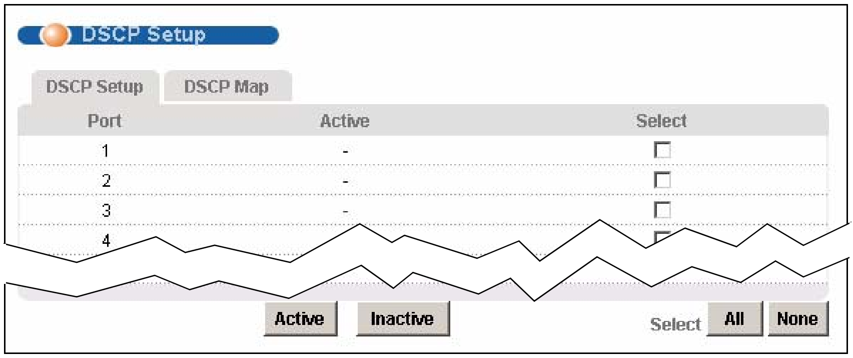
33.1 DSCP Overview

DiffServ Code Point (DSCP) is a field used for packet classification on DiffServ networks. The higher the value, the higher the priority. Lower-priority packets may be dropped if the total traffic exceeds the capacity of the network.

33.2 DSCP Setup Screen

Use this screen to activate or deactivate DSCP on each port. To open this screen, click **Advanced Application** > **DSCP**.

Figure 105 DSCP Setup



Port	Active	Select
1	-	□
2	-	□
3	-	□
4		□

The following table describes the labels in this screen.

Table 67 DSCP Setup

LABEL	DESCRIPTION
Port	This field displays each port number.
Active	This field displays whether DSCP is active (“V”) or inactive (“-”) on this port.
Select	Select this, and click **Active** or **Inactive** to enable or disable the DSCP on this port.
Active	Click this to enable DSCP on the selected ports.
Inactive	Click this to disable DSCP on the selected ports.

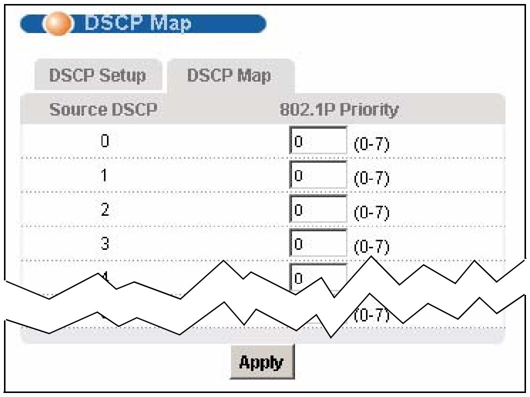
Table 67 DSCP Setup (continued)

LABEL	DESCRIPTION
All	Click this to select all entries in the table.
None	Click this to un-select all entries in the table.

33.3 DSCP Map Screen

Use this screen to convert DSCP priority to IEEE 802.1p priority. To open this screen, click **Advanced Application** > **DSCP** > **DSCP Map**.

Figure 106 DSCP Map



Source DSCP	802.1P Priority
0	0 (0-7)
1	0 (0-7)
2	0 (0-7)
3	0 (0-7)
4	0
	(0-7)

The following table describes the labels in this screen.

Table 68 DSCP Map

LABEL	DESCRIPTION
Source DSCP	This field displays each DSCP value.
802.1P Priority	Enter the IEEE 802.1p priority to which you would like to map this DSCP value.
Apply	Click **Apply** to save your changes to the IP DSLAM's volatile memory. The IP DSLAM loses these changes if it is turned off or loses power, so use the **Config Save** link on the navigation panel to save your changes to the non-volatile memory when you are done configuring.

34

TLS PVC

This chapter shows you how to set up Transparent LAN Service (VLAN stacking, Q-in-Q) on each port.

34.1 Transparent LAN Service (TLS) Overview

Transparent LAN Service (also known as VLAN stacking or Q-in-Q) allows a service provider to distinguish multiple customers VLANs, even those with the same (customer-assigned) VLAN ID, within its network.

Use TLS to add an outer VLAN tag to the inner IEEE 802.1Q tagged frames that enter the network. By tagging the tagged frames ("double-tagged" frames), the service provider can manage up to 4,094 VLAN groups with each group containing up to 4,094 customer VLANs. This allows a service provider to provide different services, based on specific VLANs, for many different customers.

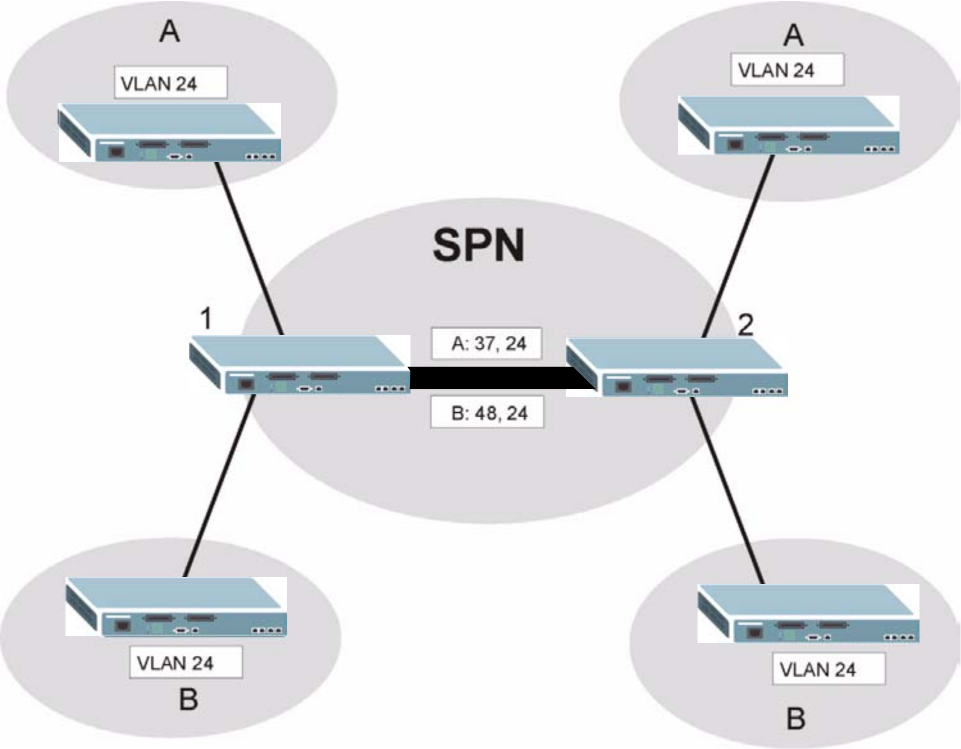
A service provider's customers may require a range of VLANs to handle multiple applications. A service provider's customers can assign their own inner VLAN tags to traffic. The service provider can assign an outer VLAN tag for each customer. Therefore, there is no VLAN tag overlap among customers, so traffic from different customers is kept separate.

Before the IP DSLAM sends the frames from the customers, the VLAN ID is added to the frames. When packets intended for specific customers are received on the IP DSLAM, the outer VLAN tag is removed before the traffic is sent.

34.1.1 TLS Network Example

In the following example figure, both A and B are Service Provider's Network (SPN) customers with VPN tunnels between their head offices and branch offices, respectively. Both have an identical VLAN tag for their VLAN group. The service provider can separate these two VLANs within its network by adding tag 37 to distinguish customer A and tag 48 to distinguish customer B at edge device 1 and then stripping those tags at edge device 2 as the data frames leave the network.

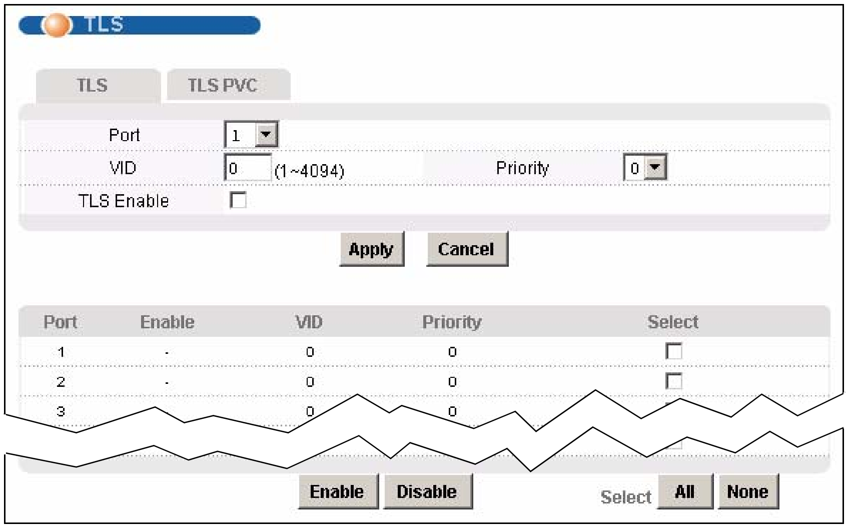
Figure 107 Transparent LAN Service Network Example



34.2 TLS Screen

Use this screen to set up Transparent LAN Services on each port. This is set up by creating a TLS PVC. See Chapter 16 on page 99 for background information about creating PVCs. To open this screen, click **Advanced Application** > **TLS**.

Figure 108 TLS



Port	1		
VID	0 (1~4094)	Priority	0
TLS Enable	□		

Port	Enable	VID	Priority	Select
1	-	0	0	□
2	-	0	0	□
3		0	0	

The following table describes the labels in this screen.

Table 69 TLS

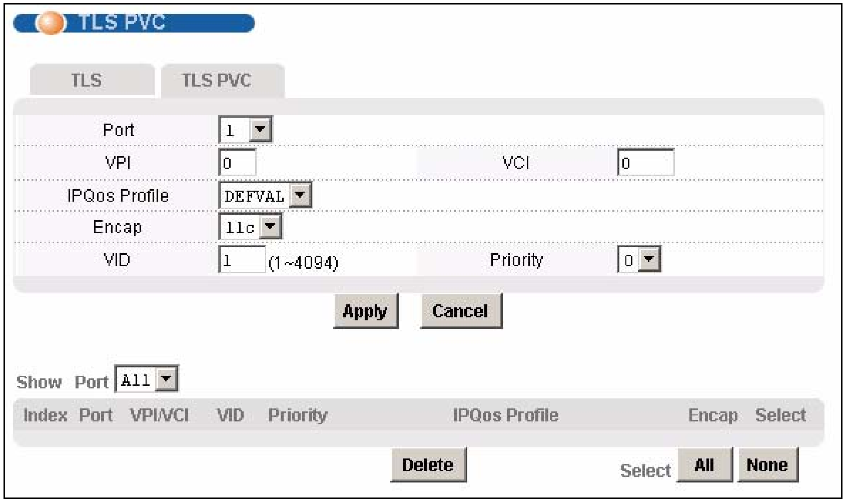
LABEL	DESCRIPTION
Port	Use this drop-down list box to select a port for which you wish to set up a TLS PVC. This field is read-only once you click on a port number below.
VID	Type a VLAN ID to assign to frames received on this channel. Note: Make sure the VID is not already used for PPPoA-to-PPPoE conversions.
Priority	Use the drop-down list box to select the priority value (0 to 7) to add to incoming frames without a (IEEE 802.1p) priority tag.
TLS Enable	Select this to enable transparent LAN service on this port.
Apply	Click this to add or save channel settings on the selected port. This saves your changes to the IP DSLAM's volatile memory. The IP DSLAM loses these changes if it is turned off or loses power, so use the **Config Save** link on the navigation panel to save your changes to the non-volatile memory when you are done configuring.
Cancel	Click **Cancel** to start configuring the screen again.
Port	This field displays the number of the xDSL port on which the PVC is configured.
Enable	This field displays "**V**" when TLS has been enabled on the xDSL port. Otherwise, it displays "**-**".
VID	This is the VLAN ID assigned to frames received on this channel.
Priority	This is the priority value (0 to 7) added to incoming frames without a (IEEE 802.1p) priority tag.
Select Delete	Select the check box in the **Select** column for an entry, and click **Delete** to remove the entry.
Select All	Click this to select all entries in the table.
Select None	Click this to un-select all entries in the table.

34.3 TLS PVC Screen

Use this screen to set up Transparent LAN Services on each port. This is set up by creating a TLS PVC. See Chapter 16 on page 99 for background information about creating PVCs. To open this screen, click **Advanced Application** > **TLS** > **TLS PVC**.

You can NOT configure PPPoA-to-PPPoE and TLS PVC settings on the same PVC.

Figure 109 TLS PVC



The following table describes the labels in this screen.

Table 70 TLS PVC

LABEL	DESCRIPTION
Port	Use this drop-down list box to select a port for which you wish to set up a TLS PVC. This field is read-only once you click on a port number below.
VPI	Type the Virtual Path Identifier for a channel on this port.
VCI	Type the Virtual Circuit Identifier for a channel on this port.
IPQos Profile	Select an IPQoS profile to classify and prioritize application traffic flowing through this TLS PVC. Use the **Basic Setting** > **xDSL Profiles Setup** > **IPQos Profile** screen to configure IPQoS profiles. See Section 17.2 on page 119.
Encap	Select an encapsulation method (**llc** or **vc**) for this TLS PVC.
VID	Type a VLAN ID to assign to frames received on this channel. Note: Make sure the VID is not already used for PPPoA-to-PPPoE conversions.
Priority	Use the drop-down list box to select the priority value (0 to 7) to add to incoming frames without a (IEEE 802.1p) priority tag.
Apply	Click this to add or save channel settings on the selected port. This saves your changes to the IP DSLAM's volatile memory. The IP DSLAM loses these changes if it is turned off or loses power, so use the **Config Save** link on the navigation panel to save your changes to the non-volatile memory when you are done configuring.
Cancel	Click **Cancel** to start configuring the screen again.
Show Port	Select which xDSL port(s) for which to display TLS PVC settings.
Index	This field displays the number of the PVC. Click a PVC's index number to use the top of the screen to edit the PVC. Note: At the time of writing, you cannot edit the VPI and VCI. If you want to change them, add a new PVC with the desired settings. Then you can delete any unwanted PVCs.
Port	This field displays the number of the xDSL port on which the PVC is configured.

Table 70 TLS PVC (continued)

LABEL	DESCRIPTION
VPI/VCI	This field displays the Virtual Path Identifier (VPI) and Virtual Circuit Identifier (VCI). The VPI and VCI identify a channel on this port.
VID	This is the VLAN ID assigned to frames received on this channel.
Priority	This is the priority value (0 to 7) added to incoming frames without a (IEEE 802.1p) priority tag.
IPQos Profile	This field displays the IPQoS profile applied for the TLS PVC.
Encap	This field displays the encapsulation method (**llc** or **vc**) configured for the TLS PVC.
Select Delete	Select the check box in the **Select** column for an entry, and click **Delete** to remove the entry.
Select All	Click this to select all entries in the table.
Select None	Click this to un-select all entries in the table.

35

Double Tagging (DT)

This chapter shows you how to configure VLAN double tagging on the IP DSLAM.

35.1 Double Tagging Overview

With Double Tagging (DT) enabled, the IP DSLAM can add two tags (C-tag and S-tag) of the VLAN ID and priority level for untagged packets received from a private network to those used in the service provider's network.

When you enable DT on a port, the port is called a DT access port. The IP DSLAM adds VLAN tags for untagged traffic but drops tagged traffic flowing through the DT access ports.

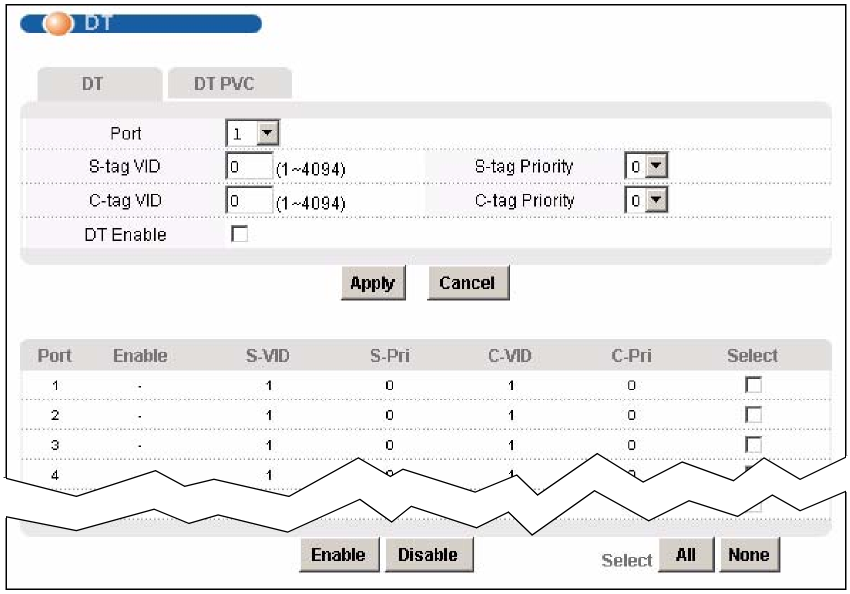
Double-tagged or single-tagged packets received on the DT access ports are dropped.

35.2 Configuring DT

Click **Advanced Application** > **DT** to open this screen.

Use this screen to view the existing DT entries. It's recommended that you add a new entry in this screen only when you want to translate untagged packets into double-tagged ones before forwarding them.

Figure 110 DT



Port	1		
S-tag VID	0 (1~4094)	S-tag Priority	0
C-tag VID	0 (1~4094)	C-tag Priority	0
DT Enable	□		

Port	Enable	S-VID	S-Pri	C-VID	C-Pri	Select
1	-	1	0	1	0	□
2	-	1	0	1	0	□
3	-	1	0	1	0	□
4		1				

The following table describes the labels in this screen.

Table 71 DT

LABEL	DESCRIPTION
Port	Use this drop-down list box to select a port for which you wish to set up a DT PVC. This field is read-only once you click on a port number below.
S-tag VID	Enter the S-tag VLAN ID from 1 to 4094. The S-tag (service tag) is the outer tag in double tagging.
S-tag Priority	Enter the S-tag priority level from 0 to 7.
C-tag VID	Enter the C-tag VLAN ID from 1 to 4094. The C-tag (customer tag) is the inner tag in double tagging.
C-tag Priority	Enter the C-tag priority level from 0 to 7.
DT Enable	Check this box to activate this entry.
Apply	Click **Apply** to insert the entry in the summary table below and save your changes to the IP DSLAM.
Cancel	Click **Cancel** to reset the fields to your previous configuration.
Port	This is the VDSL port number.
Enable	This shows whether this entry is activated or not.
S-VID	This is the S-tag VLAN ID (outer tag) to add to the untagged packets.
S-Pri	This is the S-tag priority level to add to the untagged packets.
C-VID	This is the C-tag VLAN ID to add to the untagged packets.
C-Pri	This is the C-tag priority level to add to the untagged packets.
Select Enable	Select the check box in the **Select** column for an entry, and click **Enable** to activate the entry.
Select Disable	Select the check box in the **Select** column for an entry, and click **Disable** to inactivate the entry.

Table 71 DT

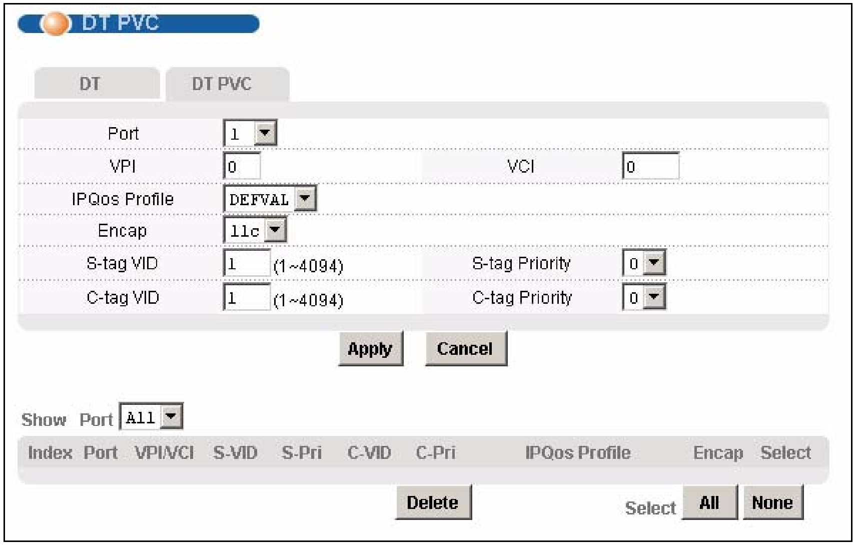
LABEL	DESCRIPTION
Select All	Click this to select all entries in the table.
Select None	Click this to un-select all entries in the table.

35.3 Configuring DT PVC

Click **Advanced Application** > **DT** > **DT PVC** to display the screen as shown.

Use this screen to view the existing DT entries. It’s recommended that you add a new entry in this screen only when you want to translate untagged packets into double-tagged ones before forwarding them.

Figure 111 DT PVC



DT PVC

Port: 1
VPI: 0　VCI: 0
IPQos Profile: DEFVAL
Encap: llc
S-tag VID: 1 (1~4094)　S-tag Priority: 0
C-tag VID: 1 (1~4094)　C-tag Priority: 0

Show Port: All

Index	Port	VPI/VCI	S-VID	S-Pri	C-VID	C-Pri	IPQos Profile	Encap	Select

The following table describes the labels in this screen.

Table 72 DT PVC

LABEL	DESCRIPTION
Port	Use this drop-down list box to select a port for which you wish to set up a DT PVC. This field is read-only once you click on a port number below.
VPI	Type the Virtual Path Identifier for a channel on this port.
VCI	Type the Virtual Circuit Identifier for a channel on this port.
IPQos Profile	Select an IPQoS profile to classify and prioritize application traffic flowing through this DT PVC. Use the **Basic Setting** > **xDSL Profiles Setup** > **IPQos Profile** screen to configure IPQoS profiles. See Section 17.2 on page 119.
Encap	Select an encapsulation method (**llc** or **vc**) for this DT PVC.
S-tag VID	Enter the S-tag VLAN ID from 1 to 4094. The S-tag (service tag) is the outer tag in double tagging.
S-tag Priority	Enter the S-tag priority level from 0 to 7.

Table 72 DT PVC

LABEL	DESCRIPTION
C-tag VID	Enter the C-tag VLAN ID from 1 to 4094. The C-tag (customer tag) is the inner tag in double tagging.
C-tag Priority	Enter the C-tag priority level from 0 to 7.
Apply	Click **Apply** to insert the entry in the summary table below and save your changes to the IP DSLAM.
Cancel	Click **Cancel** to reset the fields to your previous configuration.
Show Port	Select which xDSL port(s) for which to display DT PVC settings.
Index	This field displays the number of the PVC. Click a PVC's index number to use the top of the screen to edit the PVC. Note: At the time of writing, you cannot edit the VPI and VCI. If you want to change them, add a new PVC with the desired settings. Then you can delete any unwanted PVCs.
Port	This field displays the number of the xDSL port on which the PVC is configured.
VPI/VCI	This field displays the Virtual Path Identifier (VPI) and Virtual Circuit Identifier (VCI). The VPI and VCI identify a channel on this port.
S-VID	This is the S-tag VLAN ID (outer tag) that adds to the untagged packets.
S-Pri	This is the S-tag priority level that adds to the untagged packets.
C-VID	This is the C-tag VLAN ID that adds to the untagged packets.
C-Pri	This is the C-tag priority level that adds to the untagged packets.
IPQos Profile	This field displays the IPQoS profile applied for this DT PVC.
Encap	This field displays the encapsulation method (**llc** or **vc**) configured for the DT PVC.
Select Enable	Select the check box in the **Select** column for an entry, and click **Enable** to activate the entry.
Select Disable	Select the check box in the **Select** column for an entry, and click **Disable** to inactivate the entry.
Select All	Click this to select all entries in the table.
Select None	Click this to un-select all entries in the table.

36

ACL

This chapter shows you how to set up ACL profiles on each port.

36.1 Access Control Logic (ACL) Overview

An ACL (Access Control Logic) profile allows the IP DSLAM to classify and perform actions on the upstream traffic. Each ACL profile consists of a rule and an action, and you assign ACL profiles to PVCs.

36.1.1 ACL Profile Rules

Each ACL profile uses one of 17 rules to classify upstream traffic. These rules are listed below by rule number.

1. etype <etype> vlan <vid>
2. etype <etype> smac <mac>
3. etype <etype> dmac <mac>
4. vlan <vid> smac <mac>
5. vlan <vid> dmac <mac>
6. smac <mac> dmac <mac>
7. vlan <vid> priority <priority>
8. etype <etype>
9. vlan <vid>
10. smac <mac>
11. dmac <mac>
12. priority <priority>
13. protocol <protocol>
14. vlan <vid> srcip <ip>
15. vlan <vid> dstip <ip>
16. vlan <vid> tcp|udp srcport <port>
17. vlan <vid> tcp|udp dstport <port>

The input values for these values have the following ranges.

- <vid>: 1~4094
- <priority>: 1~7
- <etype>: 0~65535
- <protocol>: tcp|udp|ospf|igmp|ip|gre|icmp|<ptype>

- <ptype>: 0~255
- <mask>: 0~32

If you apply multiple profiles to an ADSL PVC or VDSL port, the IP DSLAM checks the profiles by rule number. The lower the rule number, the higher the priority the rule (and profile) has. For example, there are two ACL profiles assigned to a PVC. Profile1 is for VLAN ID 100 (rule number 9) traffic, and Profile2 is for IEEE 802.1p priority 0 traffic (rule number 12). The IP DSLAM checks Profile1 first. If the traffic is VLAN ID 100, the IP DSLAM follows the action in Profile1 and does not check Profile2. You cannot assign profiles that have the same rule numbers to the same ADSL PVC or VDSL port.

36.1.2 ACL Profile Actions

The IP DSLAM can perform the following actions after it classifies upstream traffic.

- rate <rate>: change the rate to the specified value (64~65472 kbps)
- rvlan <rvlan>: change the VLAN ID to the specified value (1~4094)
- rpri <rpri>: change the IEEE 802.1p priority to the specified value (0~7)
- deny: do not forward the packet

The IP DSLAM can apply more than one action to a packet, unless you select deny.

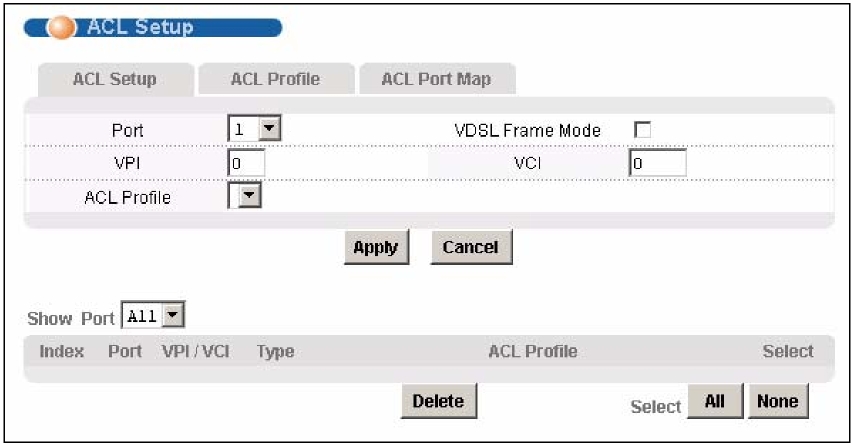
If you select the rvlan action, the IP DSLAM replaces the VLAN ID before it compares the VLAN ID of the packet to the VID of the ADSL PVC or VDSL port. As a result, it is suggested that you replace VLAN ID on super channels, not normal PVC, since super channels accept any tagged traffic. If you replace the VLAN ID for a normal ADSL PVC or VDSL port, the IP DSLAM drops the traffic because the new VLAN ID does not match the VID of the ADSL PVC or VDSL port. This is illustrated in the following scenario.

There is a normal ADSL PVC or VDSL port, and its PVID is 900. You create an ACL rule to replace the VLAN ID with 901. Initially, the traffic for the ADSL PVC or VDSL port belongs to VLAN 900. Then, the IP DSLAM checks the ACL rule and changes the traffic to VLAN 901. When the IP DSLAM finally compares the VLAN ID of the traffic (901) to the VID of the ADSL PVC or VDSL port (900), the IP DSLAM drops the packets because they do not match.

36.2 ACL Setup Screen

Use this screen to assign ACL profiles to each ADSL PVC or VDSL port. To open this screen, click **Advanced Application > ACL**.

Figure 112 ACL Setup



Port	1	VDSL Frame Mode	□
VPI	0	VCI	0
ACL Profile			

Show Port All

Index	Port	VPI / VCI	Type	ACL Profile	Select

Select

The following table describes the labels in this screen.

Table 73 ACL Setup

LABEL	DESCRIPTION
Port	Use this drop-down list box to select a port to which you wish to assign an ACL profile. This field is read-only once you click on a port number below.
VDSL Frame Mode	Select this for a VDSL port or clear this for an ADSL port.
VPI	Type the Virtual Path Identifier for a channel on this port.
VCI	Type the Virtual Circuit Identifier for a channel on this port.
ACL Profile	Use the drop-down list box to select the ACL profile you want to assign to this PVC.
Apply	Click this to save your changes to the IP DSLAM's volatile memory. The IP DSLAM loses these changes if it is turned off or loses power, so use the **Config Save** link on the navigation panel to save your changes to the non-volatile memory when you are done configuring.
Cancel	Click **Cancel** to start configuring the screen again.
Show Port	Select which xDSL port(s) for which to display ACL profile settings.
Index	This field displays the number of the ADSL PVC or VDSL port. Click an ADSL PVC or VDSL port's index number to use the top of the screen to edit the ADSL PVC or VDSL port. Note: At the time of writing, you cannot edit the VPI and VCI. If you want to change them, add a new ADSL PVC or VDSL port with the desired settings. Then you can delete any unwanted ADSL PVCs or VDSL ports.
Port	This field displays the number of the xDSL port on which the ADSL PVC or VDSL port is configured.
VPI/VCI	This field displays the Virtual Path Identifier (VPI) and Virtual Circuit Identifier (VCI). The VPI and VCI identify a channel on this port. ***** displays for a VDSL port.
Type	This field displays **PVC** for an ADSL port or ***** for a VDSL port.
ACL Profile	This field shows the ACL profile assigned to this ADSL PVC or VDSL port.
Select Delete	Select the check box in the **Select** column for an entry, and click **Delete** to remove the entry.

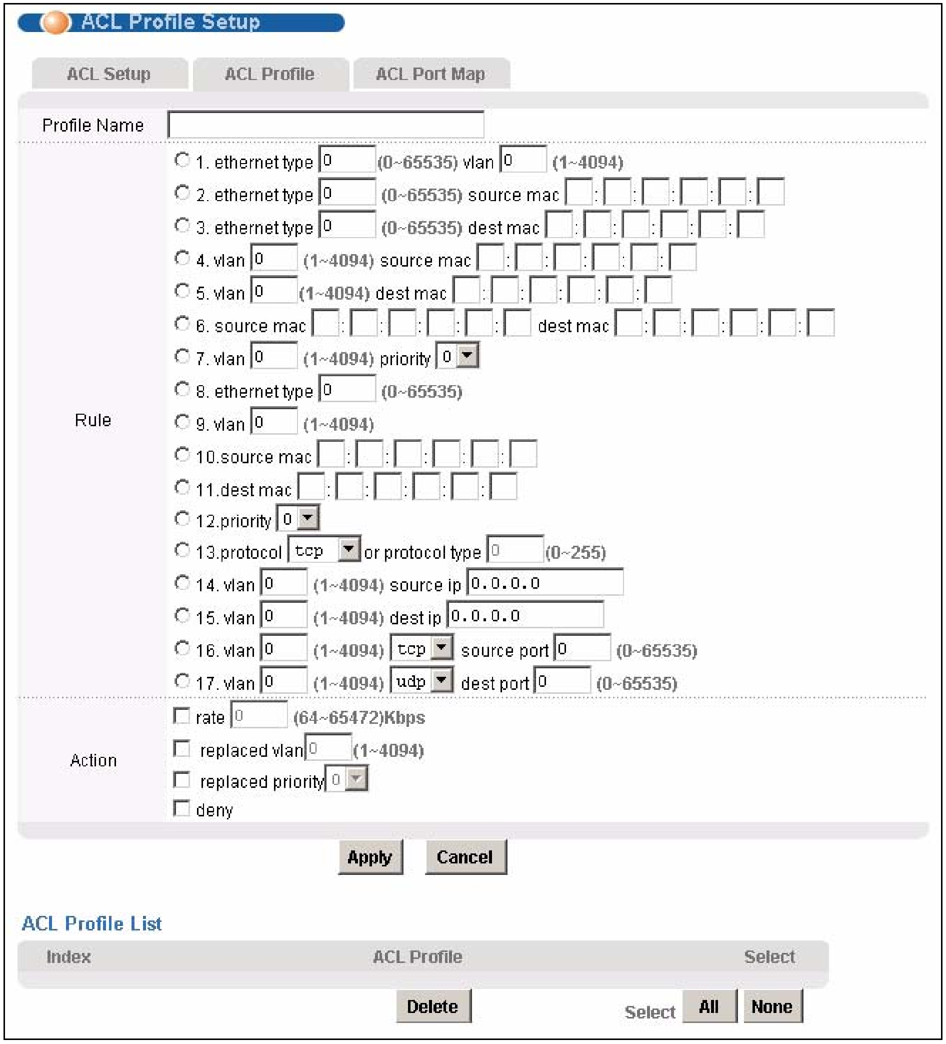
Table 73 ACL Setup (continued)

LABEL	DESCRIPTION
Select All	Click this to select all entries in the table.
Select None	Click this to un-select all entries in the table.

36.3 ACL Profile Screen

Use this screen to set up ACL profiles. To open this screen, click **Advanced Application** > **ACL** > **ACL Profile**.

Figure 113 ACL Profile



ACL Profile Setup

ACL Setup | ACL Profile | ACL Port Map

Profile Name

Rule

○ 1. ethernet type 0 (0~65535) vlan 0 (1~4094)
○ 2. ethernet type 0 (0~65535) source mac : : : : :
○ 3. ethernet type 0 (0~65535) dest mac : : : : :
○ 4. vlan 0 (1~4094) source mac : : : : :
○ 5. vlan 0 (1~4094) dest mac : : : : :
○ 6. source mac : : : : : dest mac : : : : :
○ 7. vlan 0 (1~4094) priority 0
○ 8. ethernet type 0 (0~65535)
○ 9. vlan 0 (1~4094)
○ 10.source mac : : : : :
○ 11.dest mac : : : : :
○ 12.priority 0
○ 13.protocol tcp or protocol type 0 (0~255)
○ 14. vlan 0 (1~4094) source ip 0.0.0.0
○ 15. vlan 0 (1~4094) dest ip 0.0.0.0
○ 16. vlan 0 (1~4094) tcp source port 0 (0~65535)
○ 17. vlan 0 (1~4094) udp dest port 0 (0~65535)

Action

□ rate 0 (64~65472)Kbps
□ replaced vlan 0 (1~4094)
□ replaced priority 0
□ deny

Apply | Cancel

ACL Profile List

Index	ACL Profile	Select

Delete | Select All | None

The following table describes the labels in this screen.

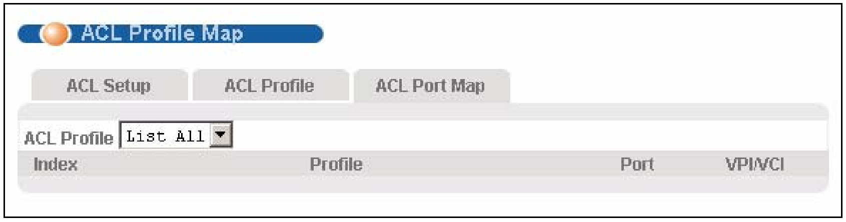
Table 74 ACL Profile

LABEL	DESCRIPTION
Profile Name	Enter a descriptive name for the ACL profile. The name can be 1-31 printable ASCII characters long. Spaces are not allowed.
Rule	Select which type of rule to use. Note: The lower the number (1-17), the higher the priority the rule has. Provide additional information required for the selected rule. Additional rules consist of one or more of the following criteria.
ethernet type	Enter the 16-bit EtherType value between 0 and 65535.
vlan	Enter a VLAN ID between 1 and 4094.
source mac	Enter the source MAC address.
dest mac	Enter the destination MAC address.
priority	Select the IEEE 802.1p priority.
protocol	Select the IP protocol used.
protocol type	Enter the IP protocol number (between 0 and 255) used.
source ip	Enter the source IP address and subnet mask in dotted decimal notation.
dest ip	Enter the source IP address and subnet mask in dotted decimal notation.
udp, tcp	Select a type of traffic (**UDP** or **TCP** protocol) for the rule.
source port	Enter the source port or range of source ports.
dest port	Enter the destination port or range of destination ports.
Action	Select which action(s) the IP DSLAM should follow when the criteria are satisfied.
rate	Select this and enter the maximum bandwidth this traffic is allowed to have.
new vlan	Select this and enter the VLAN identifier you want to use for the matched traffic.
new priority	Select the IEEE 802.1p priority to use for this traffic.
deny	Select this if you want the IP DSLAM to reject this kind of traffic.
ACL Profile List	
Index	This field displays a sequential value. The sequence in this table is not important. Click this to edit the associated ACL profile in the section above.
ACL Profile	This field displays the name of this ACL profile.
Select Delete	Select the check box in the **Select** column for an entry, and click **Delete** to remove the entry.
Select All	Click this to select all entries in the table.
Select None	Click this to un-select all entries in the table.

36.4 ACL Profile Map Screen

Use this screen to look at all the ACL profiles and the PVCs to which each one is assigned. To open this screen, click **Advanced Application** > **ACL** > **ACL Profile Map**.

Figure 114 ACL Profile Map



ACL Profile List All

Index	Profile	Port	VPI/VCI

The following table describes the labels in this screen.

Table 75 ACL Profile Map

LABEL	DESCRIPTION
ACL Profile	Select the ACL profile(s) for which you want to see which PVCs are assigned to it.
Index	This field displays the number of an entry.
Profile	This field shows the ACL profile assigned to this PVC.
Port	This field displays the ADSL port number on which the PVC is configured.
VPI/VCI	This field displays the Virtual Path Identifier (VPI) and Virtual Circuit Identifier (VCI). The VPI and VCI identify a channel on this port. ***/*** displays for VDSL ports.

37

Downstream Broadcast

This chapter shows you how to allow or block downstream broadcast traffic.

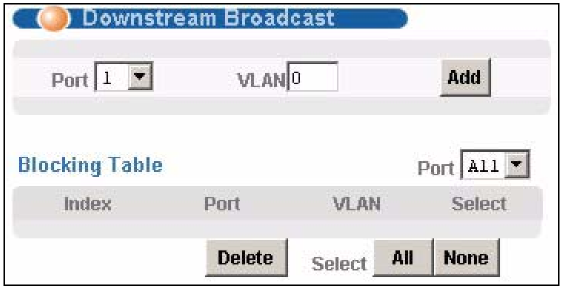
37.1 Downstream Broadcast

Downstream broadcast allows you to block downstream broadcast packets from being sent to specified VLANs on specified ports.

37.2 Downstream Broadcast Screen

To open this screen, click **Advanced Application** > **Downstream Broadcast**.

Figure 115 Downstream Broadcast



The following table describes the labels in this screen.

Table 76 Downstream Broadcast

LABEL	DESCRIPTION
Port	Use this drop-down list box to select a port for which you wish to configure settings.
VLAN	Specify the number of a VLAN (on this entry's port) to which you do not want to send broadcast traffic. The VLAN must already be configured in the system.
Add	Click **Add** to save your changes to the IP DSLAM's volatile memory. The IP DSLAM loses these changes if it is turned off or loses power, so use the **Config Save** link on the navigation panel to save your changes to the non-volatile memory when you are done configuring.
Blocking Table	
Port	Use this drop-down list box to select a port for which you wish to display settings.
Index	This field displays the number of the downstream broadcast blocking entry.

Table 76 Downstream Broadcast (continued)

LABEL	DESCRIPTION
Port	This is the number of an xDSL port through which you will block downstream broadcast traffic (on a specific VLAN).
VLAN	This field displays the number of a VLAN to which you do not want to send broadcast traffic (on the entry's port).
Select	Select an entry's **Select** check box and click **Delete** to remove the entry. Clicking **Delete** saves your changes to the IP DSLAM's volatile memory. The IP DSLAM loses these changes if it is turned off or loses power, so use the **Config Save** link on the navigation panel to save your changes to the non-volatile memory when you are done configuring.
Select All	Click **All** to mark all of the check boxes.
Select None	Click **None** to un-mark all of the check boxes.

38

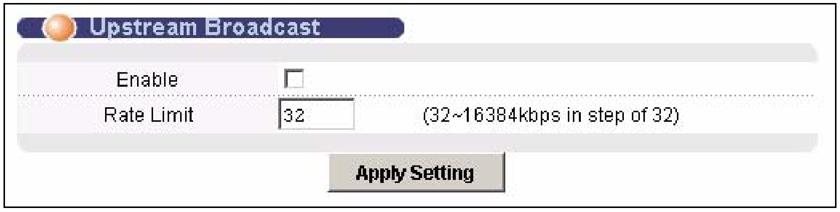
Upstream Broadcast

38.1 Upstream Broadcast Screen

Upstream broadcast allows you to define the maximum data transmission rate for upstream broadcast traffic allowed to pass through the IP DSLAM. This is useful to reduce the incoming broadcast packets and system load.

To open this screen, click **Advanced Application** > **Upstream Broadcast**.

Figure 116 Upstream Broadcast



Upstream Broadcast

Enable □

Rate Limit 32 (32~16384kbps in step of 32)

The following table describes the labels in this screen.

Table 77 Upstream Broadcast

LABEL	DESCRIPTION
Enable	Click this to enable bandwidth control for upstream broadcast traffic on the IP DSLAM.
Rate Limit	Enter the maximum bandwidth for upstream broadcast traffic (in kbps) allowed to flow into the IP DSLAM.
Apply Setting	Click **Apply Setting** to save the changes in this screen to the system's volatile memory. The system loses these changes if it is turned off or loses power, so use the **Config Save** on the navigation panel and then the **Save** button to save your changes to the non-volatile memory when you are done configuring.

39

Syslog

This chapter explains how to store your IP DSLAM's system logs to an external syslog server.

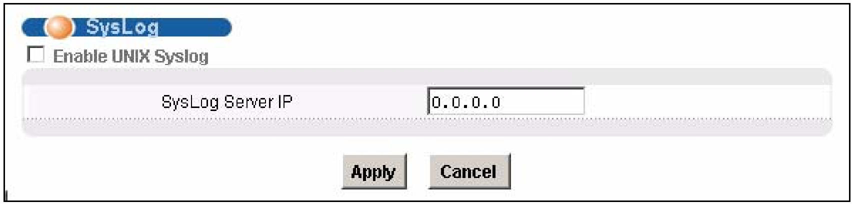
39.1 Syslog

The syslog feature sends system logs to an external syslog server.

39.2 SysLog Screen

To open this screen, click **Advanced Application** > **SysLog**.

Figure 117 SysLog



☐ Enable UNIX Syslog

SysLog Server IP: 0.0.0.0

The following table describes the labels in this screen.

Table 78 SysLog

LABEL	DESCRIPTION
Enable UNIX Syslog	Select this check box to activate syslog (system logging) and then configure the syslog parameters described in the following fields.
Syslog Server IP	Enter the IP address of the syslog server.
Apply	Click **Apply** to save your changes to the IP DSLAM's volatile memory. The IP DSLAM loses these changes if it is turned off or loses power, so use the **Config Save** link on the navigation panel to save your changes to the non-volatile memory when you are done configuring.
Cancel	Click **Cancel** to begin configuring this screen afresh.

40

Access Control

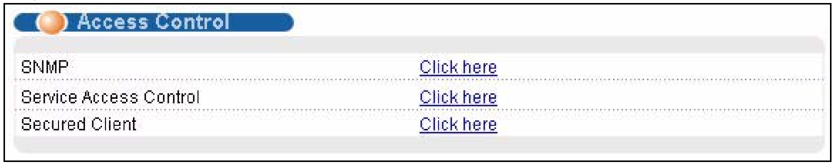
This chapter describes how to configure access control.

40.1 Access Control Screen

Use this screen to configure SNMP and enable/disable remote service access.

To open this screen, click **Advanced Application** > **Access Control**.

Figure 118 Access Control



SNMP	Click here
Service Access Control	Click here
Secured Client	Click here

40.2 Access Control Overview

A console port or Telnet session can coexist with one FTP session, a web configurator session and/or limitless SNMP access control sessions.

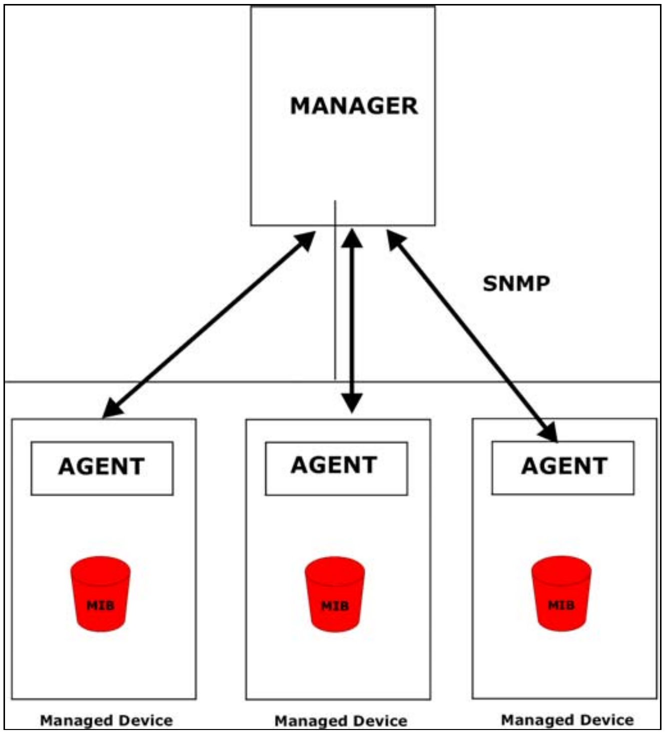
Table 79 Access Control Summary

	CONSOLE PORT	TELNET	FTP	WEB	SNMP
Number of sessions allowed	1	5	1	No limit	No limit

40.3 SNMP

Simple Network Management Protocol is a protocol used for exchanging management information between network devices. SNMP is a member of TCP/IP protocol suite. A manager station can manage and monitor the IP DSLAM through the network via SNMP version one (SNMPv1) and/or SNMP version 2c. The next figure illustrates an SNMP management operation. SNMP is only available if TCP/IP is configured.

Figure 119 SNMP Management Model



An SNMP managed network consists of two main components: agents and a manager.

An agent is a management software module that resides in a managed device (the IP DSLAM). An agent translates the local management information from the managed device into a form compatible with SNMP. The manager is the console through which network administrators perform network management functions. It executes applications that control and monitor managed devices.

The managed devices contain object variables/managed objects that define each piece of information to be collected about a device. Examples of variables include such as number of packets received, node port status etc. A Management Information Base (MIB) is a collection of managed objects. SNMP allows a manager and agents to communicate for the purpose of accessing these objects.

SNMP itself is a simple request/response protocol based on the manager/agent model. The manager issues a request and the agent returns responses using the following protocol operations:

Table 80 SNMP Commands

COMMAND	DESCRIPTION
Get	Allows the manager to retrieve an object variable from the agent.
GetNext	Allows the manager to retrieve the next object variable from a table or list within an agent. In SNMPv1, when a manager wants to retrieve all elements of a table from an agent, it initiates a Get operation, followed by a series of GetNext operations.
Set	Allows the manager to set values for object variables within an agent.
Trap	Used by the agent to inform the manager of some events.

40.3.1 Supported MIBs

MIBs let administrators collect statistics and monitor status and performance. The IP DSLAM supports the following MIBs:

- VDSL Line MIB(RFC-3728)
- MIB II IF MIB and ADSL line MIB (RFC-2662)
- SNMP MIB II (RFC-1215)
- BRIDGE MIB: FDB status
- RFC 3728 VDSL MIB

The IP DSLAM can also respond with specific data from the DSLAM private MIBs:

- dslam.mib

40.3.2 SNMP Traps

The IP DSLAM can send the following SNMP traps to an SNMP manager when an event occurs. XTUC refers to the downstream channel (for traffic going from the IP DSLAM to the subscriber). XTUR refers to the upstream channel (for traffic coming from the subscriber to the IP DSLAM).

Table 81 SNMPv2 Traps

TRAP NAME	DESCRIPTION
coldStart	This trap is sent when the IP DSLAM is turned on.
warmStart	This trap is sent when the IP DSLAM restarts.
linkDown	This trap is sent when the Ethernet link is down. Enterprise specific (xdslXtucLos) traps are sent when an xDSL link is down.
linkUp	This trap is sent when the Ethernet or xDSL link comes up.
reboot	This trap is sent when the system is going to reboot. The variable is the reason for the system reboot.
overheat	This trap is sent when the system is overheated. The variable is the current system temperature in Celsius.
overheatOver	This trap is sent when the system is no longer overheated. The variable is the current system temperature in Celsius.
fanRpmLow	This trap is sent when the RPM of the fan is too low. The variable is the current RPM of the fan.
fanRpmNormal	This trap is sent when the RPM of the fan is back within the normal range. The variable is the current RPM of the fan.
voltageOutOfRange	This trap is sent when the voltage of the system is out of the normal range. The variable is the current voltage of the system in volts.
voltageNormal	This trap is sent when the voltage of the system is back within the normal range. The variable is the current voltage of the system in volts.
extAlarmInputTrigger	This trap is sent when there is an external alarm input.
extAlarmInputRelease	This trap is sent when the external alarm input stops.
thermalSensorFailure	This trap is sent when the thermal sensor fails.
vdslPerfLofsThreshNotification	The number of times a Loss Of Frame has occurred within 15 minutes for the XTUC has reached the threshold.
vdslPerfLossThreshNotification	The number of times a Loss Of Signal has occurred within 15 minutes for the XTUC has reached the threshold.

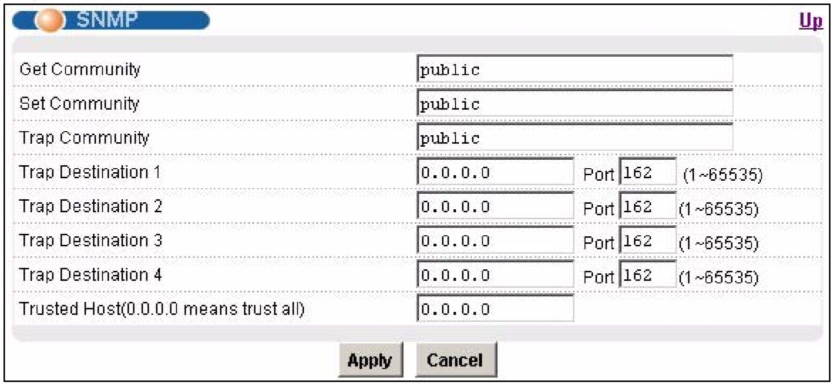
Table 81 SNMPv2 Traps (continued)

TRAP NAME	DESCRIPTION
vdslPerfLprsThreshNotification	The number of times a Loss Of Power has occurred within 15 minutes for the XTUC has reached the threshold.
vdslPerfLolsThreshNotification	The number of times a Loss Of Link has occurred within 15 minutes for the XTUC has reached the threshold.
vdslPerfESsThreshNotification	The number of error seconds within 15 minutes for the XTUC has reached the threshold.
vdslPerfSESsThreshNotification	The number of severely errored seconds within 15 minutes for the XTUC has reached the threshold.
vdslPerfUASsThreshNotification	The number of Unavailable seconds within 15 minutes for the XTUC has reached the threshold.
sysMacAntiSpoofing	The IP DSLAM has detected the same MAC address on more than one subscriber port.
alarmRisingThreshold	RMON (Remote Network Monitoring) values have exceeded the pre-defined thresholds. You can use SNMP MIB (Management Information Base) to configure the RMON thresholds. RMON is a standard to show packet statistics. Refer to RFC2819 for more information.
alarmFallingThreshold	The RMON values has returned to normal.

40.4 SNMP Screen

To open this screen, click **Advanced Application** > **Access Control** > **SNMP**.

Figure 120 SNMP



Get Community	public	
Set Community	public	
Trap Community	public	
Trap Destination 1	0.0.0.0	Port 162 (1~65535)
Trap Destination 2	0.0.0.0	Port 162 (1~65535)
Trap Destination 3	0.0.0.0	Port 162 (1~65535)
Trap Destination 4	0.0.0.0	Port 162 (1~65535)
Trusted Host(0.0.0.0 means trust all)	0.0.0.0	

The following table describes the labels in this screen.

Table 82 SNMP

LABEL	DESCRIPTION
Up	Click **Up** to go back to the previous screen.
Get Community	Enter the get community, which is the password for the incoming Get- and GetNext- requests from the management station.
Set Community	Enter the set community, which is the password for incoming Set- requests from the management station.
Trap Community	Enter the trap community, which is the password sent with each trap to the SNMP manager.

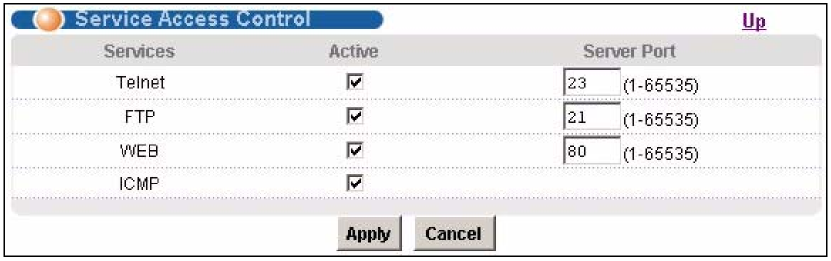
Table 82 SNMP (continued)

LABEL	DESCRIPTION
Trap Destination 1~4 Port	Enter the IP address of a station to send your SNMP traps to. Enter the port number upon which the station listens for SNMP traps.
Trusted Host	A “trusted host” is a computer that is allowed to use SNMP with the IP DSLAM. **0.0.0.0** allows any computer to use SNMP to access the IP DSLAM. Specify an IP address to allow only the computer with that IP address to use SNMP to access the IP DSLAM.
Apply	Click **Apply** to save your changes to the IP DSLAM’s volatile memory. The IP DSLAM loses these changes if it is turned off or loses power, so use the **Config Save** link on the navigation panel to save your changes to the non-volatile memory when you are done configuring.
Cancel	Click **Cancel** to begin configuring this screen afresh.

40.5 Service Access Control Screen

To open this screen, click **Advanced Application** > **Access Control** > **Service Access Control**.

Figure 121 Service Access Control



Service Access Control

Up

Services	Active	Server Port
Telnet	☑	23 (1-65535)
FTP	☑	21 (1-65535)
WEB	☑	80 (1-65535)
ICMP	☑	

The following table describes the labels in this screen.

Table 83 Service Access Control

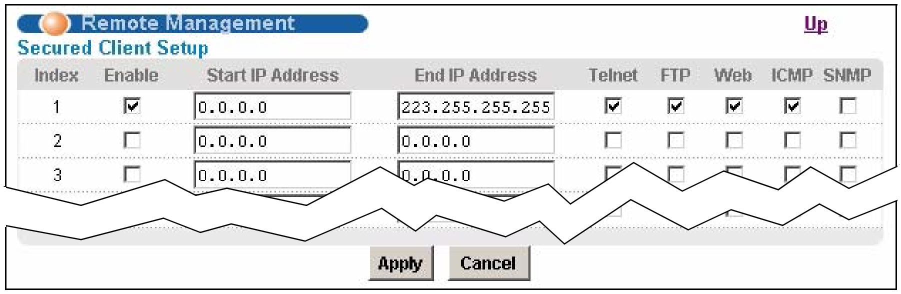
LABEL	DESCRIPTION
Up	Click **Up** to go back to the previous screen.
Services	Services you may use to access the IP DSLAM are listed here.
Active	Select the **Active** check boxes for the corresponding services that you want to allow to access the IP DSLAM.
Server Port	For Telnet, FTP or web services, you may change the default service port by typing the new port number in the **Server Port** field. If you change the default port number then you will have to let people (who wish to use the service) know the new port number for that service.
Apply	Click **Apply** to save your changes to the IP DSLAM’s volatile memory. The IP DSLAM loses these changes if it is turned off or loses power, so use the **Config Save** link on the navigation panel to save your changes to the non-volatile memory when you are done configuring.
Cancel	Click **Cancel** to begin configuring this screen afresh.

40.6 Remote Management Screen

Use this screen to configure the IP address ranges of trusted computers that may manage the IP DSLAM.

To open this screen, click **Advanced Application** > **Access Control** > **Secured Client**.

Figure 122 Remote Management (Secured Client Setup)



Remote Management

Up

Secured Client Setup

Index	Enable	Start IP Address	End IP Address	Telnet	FTP	Web	ICMP	SNMP
1	☑	0.0.0.0	223.255.255.255	☑	☑	☑	☑	☐
2	☐	0.0.0.0	0.0.0.0	☐	☐	☐	☐	☐
3	☐	0.0.0.0	0.0.0.0	☐	☐	☐	☐	☐

Apply Cancel

The following table describes the labels in this screen.

Table 84 Remote Management (Secured Client Setup)

LABEL	DESCRIPTION
Up	Click **Up** to go back to the previous screen.
Index	This is the client set index number. A “client set” is a group of one or more “trusted computers” from which an administrator may use a service to manage the IP DSLAM.
Enable	Select this check box to activate this secured client set. Clear the check box if you wish to temporarily disable the set without deleting it.
Start IP Address End IP Address	Configure the IP address range of trusted computers from which you can manage the IP DSLAM. The IP DSLAM checks if the client IP address of a computer requesting a service or protocol matches the range set here. The IP DSLAM immediately disconnects the session if it does not match.
Telnet/FTP/Web/ ICMP/SNMP	Select services that may be used for managing the IP DSLAM from the specified trusted computers.
Apply	Click **Apply** to save your changes to the IP DSLAM’s volatile memory. The IP DSLAM loses these changes if it is turned off or loses power, so use the **Config Save** link on the navigation panel to save your changes to the non-volatile memory when you are done configuring.
Cancel	Click **Cancel** to begin configuring this screen afresh.

41

PPPoE Intermediate Agent

This chapter describes how the IP DSLAM gives a PPPoE termination server additional information that the server can use to identify and authenticate a PPPoE client.

41.1 PPPoE Intermediate Agent Tag Format

If the PPPoE Intermediate Agent is enabled, the IP DSLAM adds a vendor-specific tag to PADI (PPPoE Active Discovery Initialization) and PADR (PPPoE Active Discovery Request) packets from PPPoE clients. This tag is defined in RFC 2516 and has the following format for this feature.

Table 85 PPPoE Intermediate Agent Vendor-specific Tag Format

Tag_Type (0x0105)	Tag_Len	Value	i1	i2

The Tag_Type is 0x0105 for vendor-specific tags, as defined in RFC 2516. The Tag_Len indicates the length of Value, i1 and i2. The Value is the 32-bit number 0x00000DE9, which stands for the “ADSL Forum” IANA entry. i1 and i2 are PPPoE intermediate agent sub-options, which contain additional information about the PPPoE client. The IP DSLAM supports two formats for the PPPoE intermediate agent sub-options: private and TR-101.

41.1.0.1 Private Format

There are two types of sub-option: “Agent Circuit ID Sub-option” and “Agent Remote ID Sub-option”. They have the following formats.

Table 86 PPPoE Intermediate Agent Vendor-specific Tag Format

SubOpt (0x01)	Length	Slot ID (1 byte)	Port No (1 byte)	VLAN ID (2 bytes)	Extra Information (0~23 bytes)

Table 87 PPPoE Intermediate Agent Remote ID Sub-option Format

SubOpt (0x02)	Length	MAC (6 bytes)

The IP DSLAM adds the slot ID of the PPPoE client, the port number of the PPPoE client, the VLAN ID on the PPPoE packet, and any extra information (for example, the device name) into the Agent Circuit ID Sub-option. In addition, the IP DSLAM puts the PPPoE client’s MAC address into the Agent Remote ID Sub-option. The slot ID is zero, if this value is not applicable. If the IP DSLAM adds extra information, it does not append a trailing 0x00 (00h).

41.1.0.2 TR-101 Format

The PPPoE Intermediate Agent sub-option includes the system name or IP address, slot ID, port number, VPI, and VCI on which the TCP/IP configuration request was received.

The following figure shows the format of the TR-101 PPPoE Intermediate Agent sub-option. The 1 in the first field identifies this as an Agent Circuit ID sub-option. The next field specifies the length of the field. The hostname field displays the system name, if it has been configured, the extra information field (A) if the hostname was not configured, or the IP address in dotted decimal notation (w.x.y.z), if neither the system name nor the extra information field was been configured. In either case, the hostname is truncated to 23 characters, and trailing spaces are discarded. The hostname field is followed by a space, the string “atm”, and another space. Then, a 1-byte Slot ID field specifies the ingress slot number, and a 1-byte Port No field specifies the ingress port number. Next, the VPI and VCI denote the virtual circuit that received the PPPoE message from the subscriber.

The slot ID, port number, VPI, VCI are separated from each other by a forward slash (/) colon (:) or period (.). An example is “SYSNAME atm 0/10:0.33”.

Table 88 PPPoE Intermediate Agent Sub-option Format: TR-101 for VDSL

1	N	hostname / A / IP	“ eth “	Slot ID	/	Port No.

Table 89 PPPoE Intermediate Agent Sub-option Format: TR-101 for ADSL

1	N	hostname / A / IP	“ atm “	Slot ID	/	Port No.	:	VPI	.	VCI

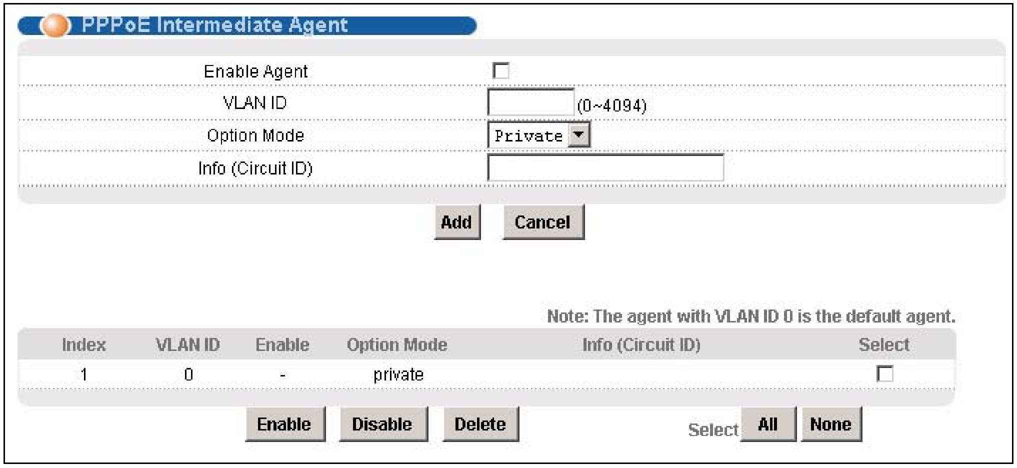
Unlike the private format for PPPoE intermediate agent, the TR-101 format for PPPoE intermediate agent does not include the Remote ID Sub-option.

41.2 PPPoE Intermediate Agent Screen

Use this screen to configure the IP DSLAM to give a PPPoE termination server additional information that the server can use to identify and authenticate a PPPoE client.

To open this screen, click **Advanced Application** > **PPPoE Intermediate Agent**.

Figure 123 PPPoE Intermediate Agent



PPPoE Intermediate Agent

Enable Agent	□
VLAN ID	(0~4094)
Option Mode	Private
Info (Circuit ID)	

Note: The agent with VLAN ID 0 is the default agent.

Index	VLAN ID	Enable	Option Mode	Info (Circuit ID)	Select
1	0	-	private		□

The following table describes the labels in this screen.

Table 90 PPPoE Intermediate Agent

LABEL	DESCRIPTION
Enable Agent	Select this if you want the IP DSLAM to add a vendor-specific tag to PADI (PPPoE Active Discovery Initiation) and PADR (PPPoE Active Discovery Request) packets from PPPoE clients in the specified VLAN. This tag contains information that a PPPoE termination server can use to identify and authenticate a PPPoE client. This information includes the slot ID, port number, VLAN ID, and MAC address of the PPPoE client, as well as any additional information specified in the **Info** field. Clear this if you do not want the IP DSLAM to add a vendor-specific tag to PADI and PADR packets from PPPoE clients in the specified VLAN.
VLAN ID	Enter the source VLAN ID for which the PPPoE intermediate agent settings apply. Enter **0** if you want to configure the default settings for all VLAN.
Option Mode	Select either **Private** or **TR-101** PPPoE Intermediate Agent sub-option.
Info (Circuit ID)	Enter any extra information the IP DSLAM adds to PADI and PADR packets in the specified VLAN. You can enter up to 23 printable ASCII characters or spaces.
Add	Click **Add** to save the settings. The settings then display in the summary table at the bottom of the screen. Clicking **Add** saves your changes to the IP DSLAM’s volatile memory. The IP DSLAM loses these changes if it is turned off or loses power, so use the **Config Save** link on the navigation panel to save your changes to the non-volatile memory when you are done configuring.
Cancel	Click **Cancel** to begin configuring the fields afresh.
Index	This field displays the index number of the entry.
VLAN ID	This field displays the source VLAN ID for which the PPPoE intermediate agent settings apply.
Enable	This field displays whether or not the IP DSLAM adds a vendor-specific tag to PADI (PPPoE Active Discovery Initiation) and PADR (PPPoE Active Discovery Request) packets from PPPoE clients in the specified VLAN.
Info (Circuit ID)	This field displays any extra information the IP DSLAM adds to PADI and PADR packets in the specified VLAN, if the PPPoE intermediate agent is turned on.
Select Enable	Select the check box in the **Select** column for an entry, and click **Enable** to add a vendor-specific tag to PADI and PADR packets for PPPoE clients in the selected VLAN(s).
Select Disable	Select the check box in the **Select** column for an entry, and click **Disable** to not add a vendor-specific tag to PADI and PADR packets for PPPoE clients in the selected VLAN(s).
Select Delete	Select the check box in the **Select** column for an entry, and click **Delete** to delete the PPPoE intermediate agent settings for subscribers in the selected VLAN(s). This also disables this feature for PPPoE clients in the selected VLAN(s).
Select All	Click **All** to mark all of the check boxes.
Select None	Click **None** to deselect all of the check boxes.

42

MTU Size

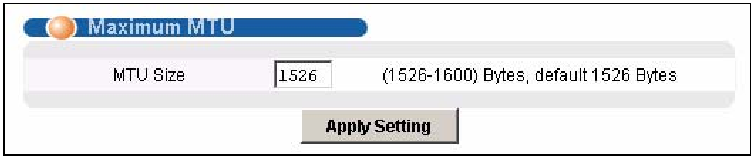
This chapter describes how to configure the Maximum Transmission Unit (MTU) for the Ethernet interfaces. The Ethernet interfaces discard any packets larger than this.

42.1 MTU Size Screen

Use this screen to configure the Maximum Transmission Unit (MTU) for the Ethernet interfaces. The Ethernet interfaces discard any packets larger than this.

To open this screen, click **Advanced Application** > **MTU Size**.

Figure 124 MTU



Maximum MTU

MTU Size: 1526 (1526-1600) Bytes, default 1526 Bytes

The following table describes the labels in this screen.

Table 91 MTU

LABEL	DESCRIPTION
MTU Size	Enter the size, in bytes, of the Maximum Transmission Unit (MTU) for the Ethernet interfaces. The Ethernet interfaces discard any packets larger than this.
Apply Setting	Click **Apply Setting** to save your MTU settings. Clicking **Apply Setting** saves your changes to the IP DSLAM's volatile memory. The IP DSLAM loses these changes if it is turned off or loses power, so use the **Config Save** link on the navigation panel to save your changes to the non-volatile memory when you are done configuring.

43

OUI Filter

This chapter describes how to configure a filter rule for each subscriber port to stop the IP DSLAM from forwarding traffic from specified devices based on OUI (Organizationally Unique Identifier).

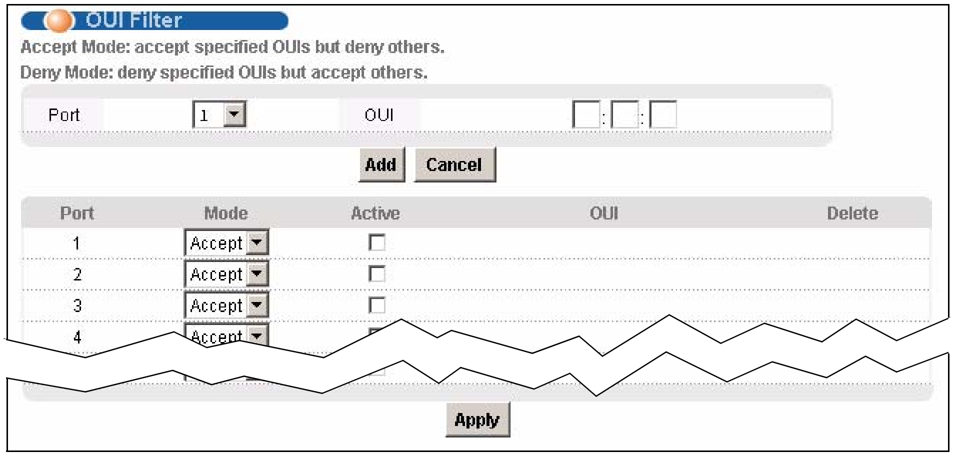
43.1 The OUI Filter Screen

Configure an OUI (Organizationally Unique Identifier) filter to block or forward packets from devices with the specified OUI in the MAC address.

The OUI field is the first three octets in a MAC address. An OUI uniquely identifies the manufacturer of a network device and allows you to identify from which device brands the switch will accept traffic or send traffic to. The OUI value is assigned by the IANA.

Click **Advanced Application** > **OUI Filter** to display the following screen.

Figure 125 OUI Filter



OUI Filter

Accept Mode: accept specified OUIs but deny others.

Deny Mode: deny specified OUIs but accept others.

Port	1	OUI	□:□:□

Add Cancel

Port	Mode	Active	OUI	Delete
1	Accept	□		
2	Accept	□		
3	Accept	□		
4	Accept	□		

Apply

The following table describes the labels in this screen.

Table 92 OUI Filter

LABEL	DESCRIPTION
Port	Select a port for which you wish to configure packet type filtering.
OUI	Enter the first three octets of a MAC address in the format xx:xx:xx. For example, 00:AF:FF.
Add	Click this to save the **OUI** to the specified port.
Cancel	Click this to reset the **OUI** field.

Table 92 OUI Filter (continued)

LABEL	DESCRIPTION
Port	This displays the IP DSLAM’s port number.
Mode	Specify the action on matched frames. Select **Accept** to allow frames with a matched OUI field in the MAC addresses. The switch blocks frames with other OUIs not specified. Select **Deny** to block frames with a matched OUI field in the MAC addresses. The switch allows frames with other OUIs not specified.
Active	Select this to activate this filter. Clear this check box to disable the filter without deleting it.
OUI	This displays the first three octets of a MAC address in the format xx:xx:xx.
Delete	Click this to remove the OUI filter from the port.
Apply	Click **Apply** to save the changes in this screen to the system’s volatile memory. The system loses these changes if it is turned off or loses power, so use the **Config Save** on the navigation panel and then the **Save** button to save your changes to the non-volatile memory when you are done configuring.

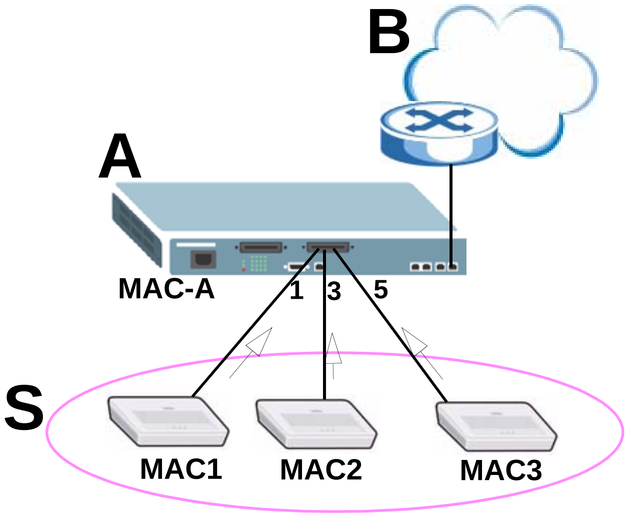
N1MAC

44.1 Overview

N1MAC is multiple-to-one MAC address conversion. N1MAC allows the IP DSLAM (**A**) to replace the MAC addresses of subscriber xDSL modems (**S**) with the IP DSLAM's MAC address in upstream packets. This removes the need to maintain a big MAC address table and prevents MAC spoofing attacks on central devices behind the IP DSLAM.

In this example, N1MAC is enabled on ports **1**, **3** and **5** for traffic forwarded from three VDSL modems. **A** replaces subscriber xDSL modem MAC addresses (**MAC1**, **MAC2** and **MAC3**) with its MAC address (**MAC-A**) on a frame forwarded to the backbone network (**B**). Backbone devices only see a frame from **A** and record only **A**'s MAC address in their MAC tables.

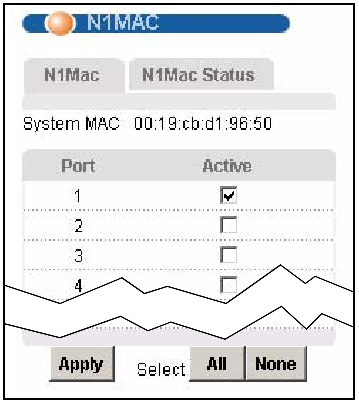
Figure 126 N1MAC



44.2 N1MAC Screen

Use this screen to enable or disable N1MAC on xDSL subscriber ports. To open this screen, click **Advanced Application** > **N1MAC**.

Figure 127 N1MAC



System MAC 00:19:cb:d1:96:50

Port	Active
1	☑
2	□
3	□
4	□

The following table describes the labels in this screen.

Table 93 N1MAC

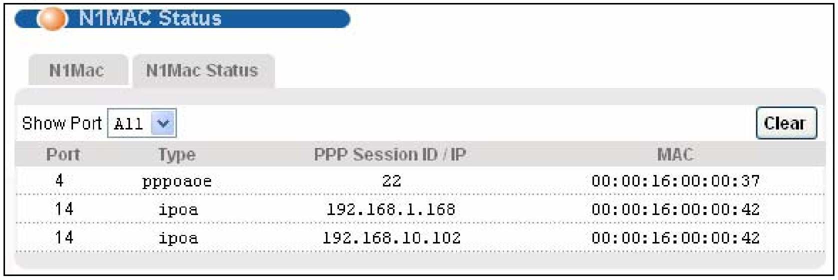
LABEL	DESCRIPTION
System MAC	This field displays the IP DSLAM's MAC address used to replace MAC addresses of subscriber xDSL modems in upstream packets.
Port	This field displays the available VDSL port numbers.
Active, Apply	Select **Active** and click **Apply** to enable N1MAC on specified port(s).
Select All	Click **All** to mark all of the check boxes.
Select None	Click **None** to deselect all of the check boxes.

44.3 N1MAC Status Screen

To open this screen, click **Advanced Application** > **N1MAC** > **N1Mac Status**.

Use this screen to check the multiple-to-one MAC mapping table for port(s).

Figure 128 N1MAC



Show Port All

Port	Type	PPP Session ID / IP	MAC
4	pppoaoe	22	00:00:16:00:00:37
14	ipoa	192.168.1.168	00:00:16:00:00:42
14	ipoa	192.168.10.102	00:00:16:00:00:42

The following table describes the labels in this screen.

Table 94 N1MAC

LABEL	DESCRIPTION
Show Port	Select a port or **All** to display the available multiple-to-one MAC mapping table for the port(s).
Clear	Click this to remove all entries shown in this screen.

Table 94 N1MAC (continued)

LABEL	DESCRIPTION
Port	This field displays an xDSL port number.
Type	This field displays **pppoaoe** when the connected subscriber uses PPPoE or PPPoA for the xDSL connection. **ipoa** or **ipoe** displays when the subscriber uses IPoA or IPoE for the connection.
PPP Session ID / IP	This field displays a PPP session identifier (when using PPPoA or PPPoE) or an IP address (when using IPoA or IPoE) the IP DSLAM uses to recognize the original subscriber’s MAC address. The IP DSLAM puts the subscriber’s MAC address back into traffic returned from the uplink network.
MAC	This field displays a MAC address which has been replaced with the IP DSLAM’s MAC address in upstream frames.

45

Dot3ad

45.1 Aggregation Switch Mode

IEEE 802.3ad link aggregation (trunking) is the grouping of physical ports into one logical higher-capacity link. You may want to trunk ports if for example, it is cheaper to use multiple lower-speed links than to under-utilize a high-speed, but more costly, single-port link.

A trunk group is one logical link containing multiple ports. The beginning port of each trunk group must be physically connected to form a trunk group.The IP DSLAM supports both static and dynamic link aggregation.

You don’t have available ports after you aggregate the two Ethernet ports on the IP DSLAM.

In a properly planned network, it is recommended to implement static link aggregation only. This ensures increased network stability and control over the trunk groups on your IP DSLAM.

45.2 Dynamic Link Aggregation

The IP DSLAM adheres to the IEEE 802.3ad standard for static and dynamic (LACP) port trunking.

The IP DSLAM supports the link aggregation IEEE802.3ad standard. This standard describes the Link Aggregation Control Protocol (LACP), which is a protocol that dynamically creates and manages trunk groups.

When you enable LACP link aggregation on a port, the port can automatically negotiate with the ports at the remote end of a link to establish trunk groups. LACP also allows port redundancy, that is, if an operational port fails, then one of the “standby” ports become operational without user intervention. Please note that:

- You must connect all ports point-to-point to the same Ethernet switch and configure the ports for LACP trunking.
- LACP only works on full-duplex links.

- All ports in the same trunk group must have the same media type, speed, duplex mode and flow control settings.

Configure trunk groups or LACP before you connect the IP DSLAM to avoid causing network topology loops.

45.2.1 Link Aggregation ID

LACP aggregation ID consists of the following information[2]:

Table 95 Link Aggregation ID: Local IP DSLAM

SYSTEM PRIORITY	MAC ADDRESS	KEY	PORT PRIORITY	PORT NUMBER
0000	00-00-00-00-00-00	0000	00	0000

Table 96 Link Aggregation ID: Peer IP DSLAM

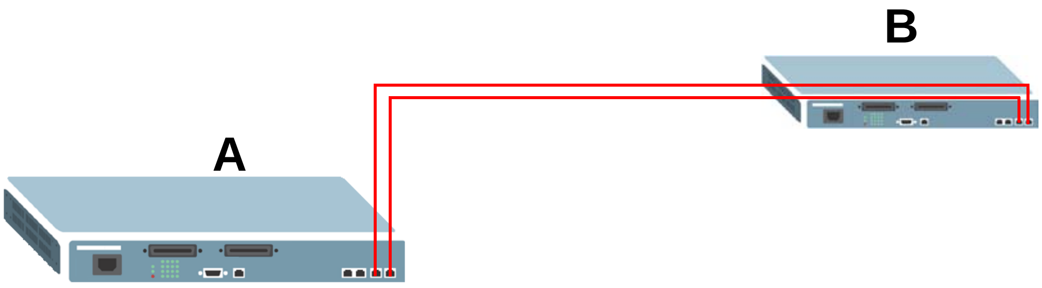
SYSTEM PRIORITY	MAC ADDRESS	KEY	PORT PRIORITY	PORT NUMBER
0000	00-00-00-00-00-00	0000	00	0000

45.3 Static Aggregation Example

This example shows you how to create a static port trunk group for Ethernet ports 1 (ENET1) and 2 (ENET2).

Make your physical connections - make sure that the ports that you want to belong to the trunk group are connected to the same destination. The following figure shows Ethernet ports 1~2 on IP DSLAM **A** connected to IP DSLAM **B**.

Figure 129 Aggregation Example - Physical Connections

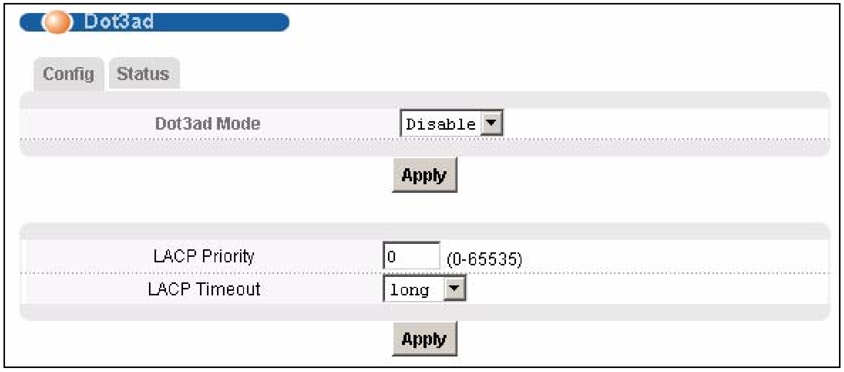


45.4 Dot3ad Screen

Click **Advanced Application** > **Dot3ad** to open the screen. Use this screen to configure IEEE 802.3ad link aggregation settings to group Ethernet ports into a trunk to increase the uplink bandwidth.

[2] Port Priority and Port Number are 0 as it is the aggregator ID for the trunk group, not the individual port.

Figure 130 Dot3ad



Dot3ad Mode: Disable

LACP Priority: 0 (0-65535)

LACP Timeout: long

The following table describes the labels in this screen.

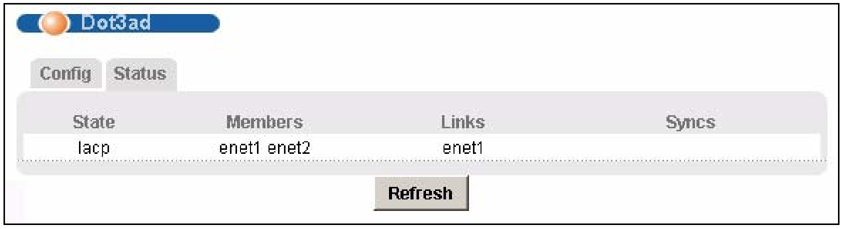
Table 97 Switch Setup Dot3ad

LABEL	DESCRIPTION
Dot3ad Mode	Select **Disable** to disable link aggregation on the IP DSLAM. Select **LACP** to use Link Aggregation Control Protocol (LACP), to dynamically create and manage the trunk group. Select **Static** to have the IP DSLAM add the two Ethernet ports into a trunk group.
Apply	Click this to save the link aggregation mode setting.
LACP Priority	Type a number between 1 and 65,535 for the LACP system priority. The IP DSLAM with the lowest system priority (and lowest port number if system priority is the same) becomes the LACP “server”. The LACP “server” controls the operation of LACP setup. Enter a number to set the priority of an active port using Link Aggregate Control Protocol (LACP). The smaller the number, the higher the priority level.
LACP Timeout	LACP timeout is the time interval between the individual port exchanges of LACP packets in order to check that the peer port in the trunk group is still up. If a port does not respond after three tries, then it is deemed to be “down” and is removed from the trunk. Set a short timeout (one second) for busy trunked links to ensure that disabled ports are removed from the trunk group as soon as possible. Select either short (1 second) or long (30 seconds).
Apply	Select this to save the LACP settings.

45.5 Dot3ad Status Screen

Click **Advanced Application** > **Dot3ad** > **Status** to open the screen. Use this screen to configure IEEE 802.3ad link aggregation settings which groups Ethernet ports into a trunk to increase the uplink bandwidth.

Figure 131 Dot3ad Status



State	Members	Links	Syncs
lacp	enet1 enet2	enet1	

The following table describes the labels in this screen.

Table 98 Dot3ad Status

LABEL	DESCRIPTION
State	This field displays the link aggregation mode configured for the Ethernet ports. **disable** displays when you disable link aggregation on the IP DSLAM. **lacp** displays when you use Link Aggregation Control Protocol (LACP), to dynamically create and manage the trunk group. **static** displays when you use static link aggregation for the trunk group.
Members	This field displays the member port(s) in the trunk group.
Links	This field displays the trunk member port(s) which has been added in the LACP group.
Syncs	This field displays port(s) which have successfully negotiated with the port at the peer end in the LACP group. Note: This field only displays values if you enable LACP on the ports at the both peer ends.

46

MAC Force Forwarding

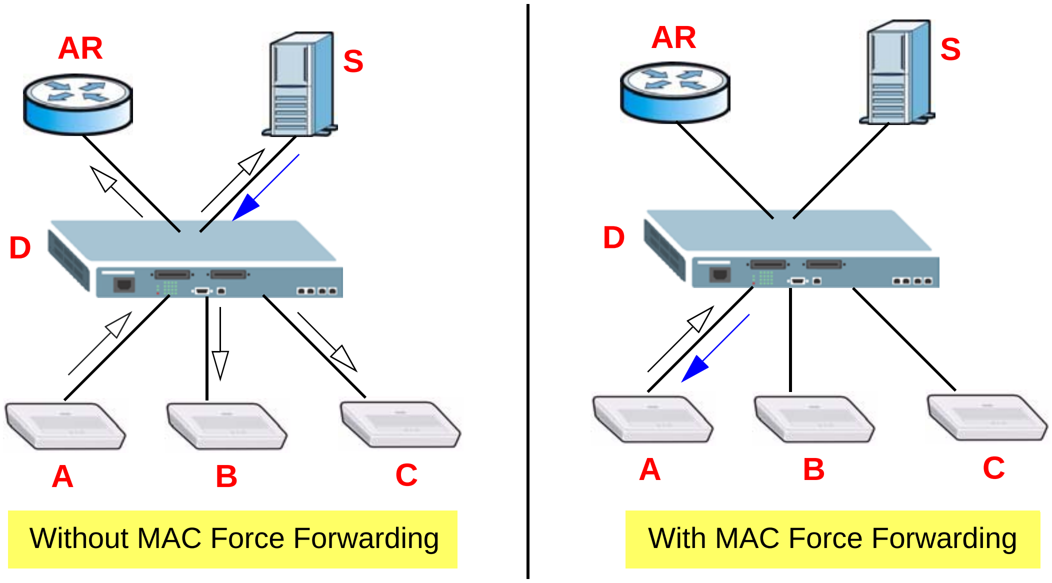
46.1 Overview

MAC force forwarding is a method used to separate subscribers for management purposes. The IP DSLAM intercepts a subscriber's ARP (Address Resolution Protocol) requests and has the subscriber send traffic to a pre-defined Access Router (AR) or Application Server (AS). The AR or AS routes or forwards subscriber traffic so the subscribers do not know the MAC addresses of servers on the network. A network administrator can use the AR or AS to monitor and manage subscriber traffic. This prevents attackers from getting MAC address information from your network and improves the network bandwidth usage performance.

An example is shown next, MAC force forwarding is disabled at the left. **A** is a subscriber who sends an ARP request to ask a server's (**S**) MAC address. All subscribers, router (**AR**), and **S** receive a copy from the IP DSLAM (**D**). **S** then replies to **A**'s request. **A** and **S** communicate directly for further data transmission. In this case, all subscribers in the network can know the servers' MAC address information.

However, with MAC force forwarding enabled (as shown next at the right), **D** will reply to **A**'s ARP request with **AR**'s MAC address. **A** sends traffic to **AR**. **AR** forwards the traffic to **S**. In this case, none of the subscribers can know **S**'s MAC address.

Figure 132 MAC Force Forwarding



46.2 MAC Force Forwarding Examples

In your network, you have the following IP assignments.

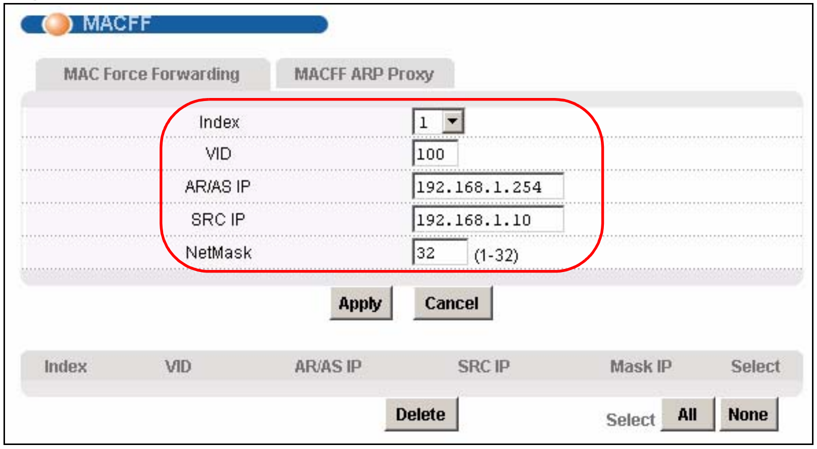
Table 99 MAC Force Forwarding Example: IP Address Settings

HOSTS	VLAN	IP ADDRESS
subscribers 1~8	100	192.168.1.10~192.168.1.18
subscribers 9~24	200	192.168.1.200~192.168.1.216
server (**S**)	100, 150, 200	192.168.1.250
access router (**AR**)	1, 100	192.168.1.254
access router 2 (**AR2**)	1, 100, 150, 200	192.168.1.253

Example 1: Source is a Single IP

If you want to force all traffic sent between subscriber 1 and the server (**S**) through **AR**, you can have the following settings in the **Advanced Application** > **MACFF** screen. Note that **32** entered in the **NetMask** field indicates a single subscriber device is included.

Figure 133 MAC Force Forwarding Configuration Example 1



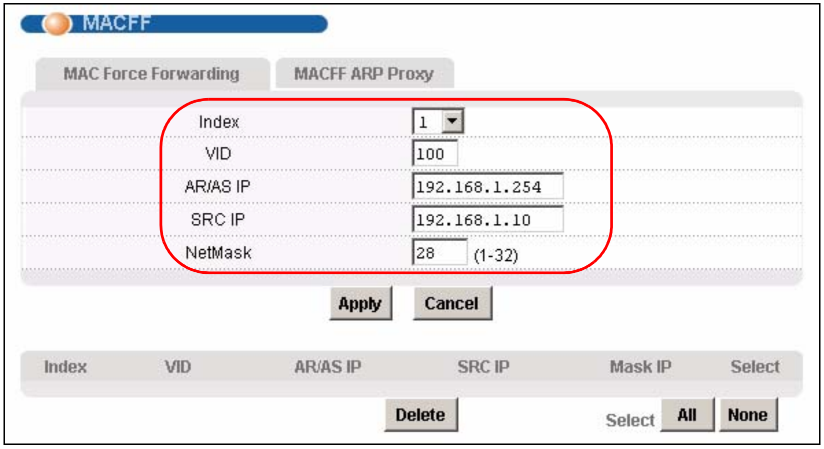
Index: 1
VID: 100
AR/AS IP: 192.168.1.254
SRC IP: 192.168.1.10
NetMask: 32 (1-32)

Example 2: Source is a Range of IPs or a Subnet

If you want to force all traffic between subscribers 1~8 and the server (**S**) to go through **AR**, you can have the following settings. Note that **28** entered in the **NetMask** field indicates fifteen subscriber devices are included.

You have to calculate the netmask depending on the number of IP addresses you want to include in a MAC force forwarding rule.

Figure 134 MAC Force Forwarding Configuration Example 2

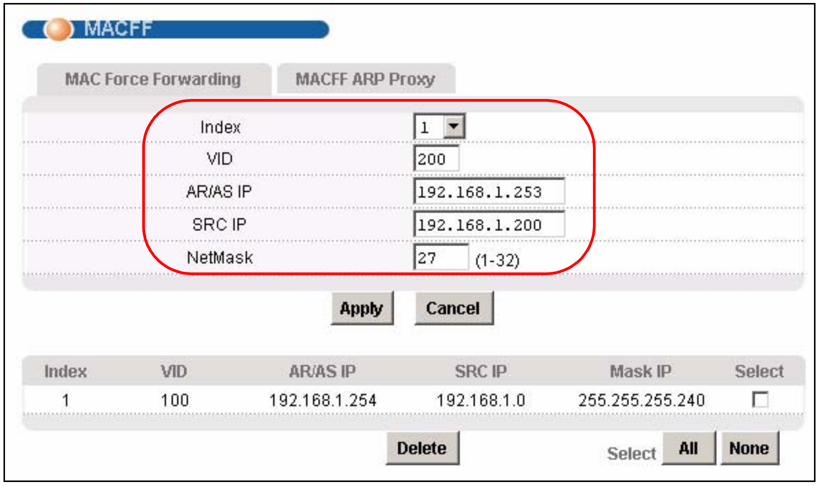


Index	1
VID	100
AR/AS IP	192.168.1.254
SRC IP	192.168.1.10
NetMask	28 (1-32)

Index	VID	AR/AS IP	SRC IP	Mask IP	Select

Furthermore, if you want to force all traffic between subscribers 9~16 and the server (**S**) through **AR2**, you can add one more rule as shown. Note that **27** entered in the **NetMask** field indicates that thirty-one subscriber devices are included. You can then monitor separated traffic centrally on **AR** or **AR2**.

Figure 135 MAC Force Forwarding Configuration Example 3



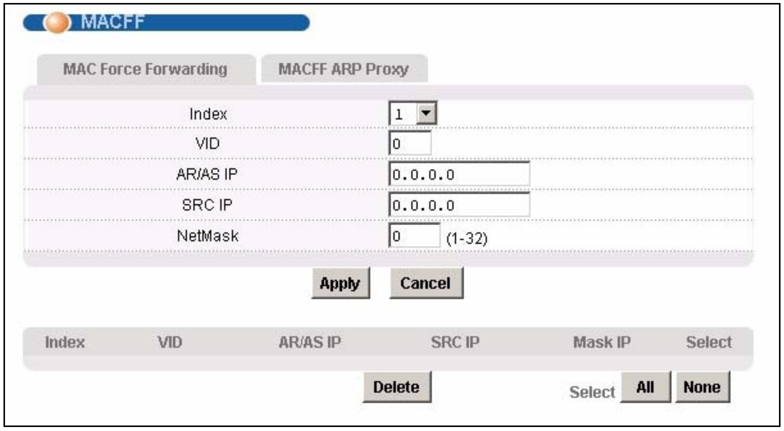
Index	1
VID	200
AR/AS IP	192.168.1.253
SRC IP	192.168.1.200
NetMask	27 (1-32)

Index	VID	AR/AS IP	SRC IP	Mask IP	Select
1	100	192.168.1.254	192.168.1.0	255.255.255.240	□

46.3 MACFF Screen

Click **Advanced Application** > **MACFF** to open the screen. Use this screen to configure the MAC force forwarding settings.

Figure 136 MAC Force Forwarding



Index	1
VID	0
AR/AS IP	0.0.0.0
SRC IP	0.0.0.0
NetMask	0 (1-32)

The following table describes the labels in this screen.

Table 100 MAC Force Forwarding

LABEL	DESCRIPTION
Index	Select an index number for the rule you want to configure below. This index number determines the order in which the IP DSLAM checks the rules.
VID	Enter the VLAN ID of the subscribers for which you are configuring this rule.
AR/AS IP	Enter an AR (Access Router) or AS (Application Server) IP address. Note: This router or server should also be a member of the specified VLAN.
SRC IP	Enter a possible source IP address of your subscriber device(s).
NetMask	Enter the number of bits for the specified IP address's netmask from left to right. This determines how many subscriber IP addresses should be included in this rule. See Network Size and Notation on page 245 if you do not know how to set this.
Apply	Click **Apply** to save the settings in this section. The settings then display in the summary table at the bottom of the screen. Clicking **Apply** saves your changes to the IP DSLAM's volatile memory. The IP DSLAM loses these changes if it is turned off or loses power, so use the **Config Save** link on the navigation panel to save your changes to the non-volatile memory when you are done configuring.
Cancel	Click **Cancel** to begin configuring the fields afresh.
Index	This field displays the index number of an entry.
VID	This field displays the VLAN ID to which the rule is applied.
AR/AS IP	This field displays the IP address of an Access Router (AR) or Application Server (AS). The IP DSLAM replies to the subscriber ARP requests with this device's MAC address.
SRC IP	This field displays the subscriber IP network of a rule.
Mask IP	This field displays the netmask for the subscriber IP network.
Select	Select this, and click **Delete** to remove the setting.
Delete	Click this to remove the selected setting(s).
Select All	Click this to select all entries in the table.
Select None	Click this to un-select all entries in the table.

Network Size

The size of the network number determines the maximum number of possible hosts you can have on your network. The larger the number of network number bits, the smaller the number of remaining host ID bits.

An IP address with host IDs of all zeros is the IP address of the network (192.168.1.0 with a 24-bit subnet mask, for example). An IP address with host IDs of all ones is the broadcast address for that network (192.168.1.255 with a 24-bit subnet mask, for example).

As these two IP addresses cannot be used for individual hosts, calculate the maximum number of possible hosts in a network as follows:

Table 101 Maximum Host Numbers

SUBNET MASK		HOST ID SIZE		MAXIMUM NUMBER OF HOSTS
8 bits	255.0.0.0	24 bits	$2^{24} – 2$	16777214
16 bits	255.255.0.0	16 bits	$2^{16} – 2$	65534
24 bits	255.255.255.0	8 bits	$2^{8} – 2$	254
29 bits	255.255.255.248	3 bits	$2^{3} – 2$	6

Notation

Since the mask is always a continuous number of ones beginning from the left, followed by a continuous number of zeros for the remainder of the 32 bit mask, you can simply specify the number of ones instead of writing the value of each octet. This is usually specified by writing a “/” followed by the number of bits in the mask after the address.

For example, 192.1.1.0 /25 is equivalent to saying 192.1.1.0 with subnet mask 255.255.255.128.

The following table shows some possible subnet masks using both notations.

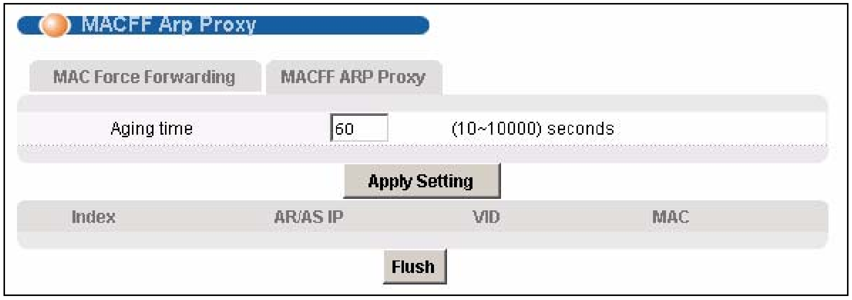
Table 102 Alternative Subnet Mask Notation

SUBNET MASK	ALTERNATIVE NOTATION	LAST OCTET (BINARY)	LAST OCTET (DECIMAL)
255.255.255.0	/24	0000 0000	0
255.255.255.128	/25	1000 0000	128
255.255.255.192	/26	1100 0000	192
255.255.255.224	/27	1110 0000	224
255.255.255.240	/28	1111 0000	240
255.255.255.248	/29	1111 1000	248
255.255.255.252	/30	1111 1100	252

46.4 MACFF ARP Proxy Screen

Click **Advanced Application > MACFF Arp Proxy** to open the screen. Use this screen to configure an expiration time for configured Access Router (AR) and Application Server (AS) ARP table entries. See Section 46.3 on page 243.

Figure 137 MAC ARP Proxy



Aging time 60 (10~10000) seconds

The following table describes the labels in this screen.

Table 103 MAC ARP Proxy

LABEL	DESCRIPTION
Aging time	Enter a number of seconds (10~10000) to set how long the IP DSLAM keeps the MAC ARP proxy table's entries of configured AR and AS devices if subscribers no longer query them within this time. Enter 0 to disable the aging time.
Apply Setting	Click **Apply Setting** to save your changes to the IP DSLAM's volatile memory. The IP DSLAM loses these changes if it is turned off or loses power, so use the **Config Save** link on the navigation panel to save your changes to the non-volatile memory when you are done configuring.
Index	This field displays the index number of a MAC address entry.
AR/AS IP	This field displays the IP address of a configured AR or AS. See Section 46.3 on page 243.
VID	This field displays the VLAN ID of the AR or AS.
MAC	This field displays the AR's or AS's MAC address the IP DSLAM has learned.
Flush	Click **Flush** to remove all of the entries from this MAC ARP proxy table.

PART IV

Routing Protocol, Alarm and Management

47

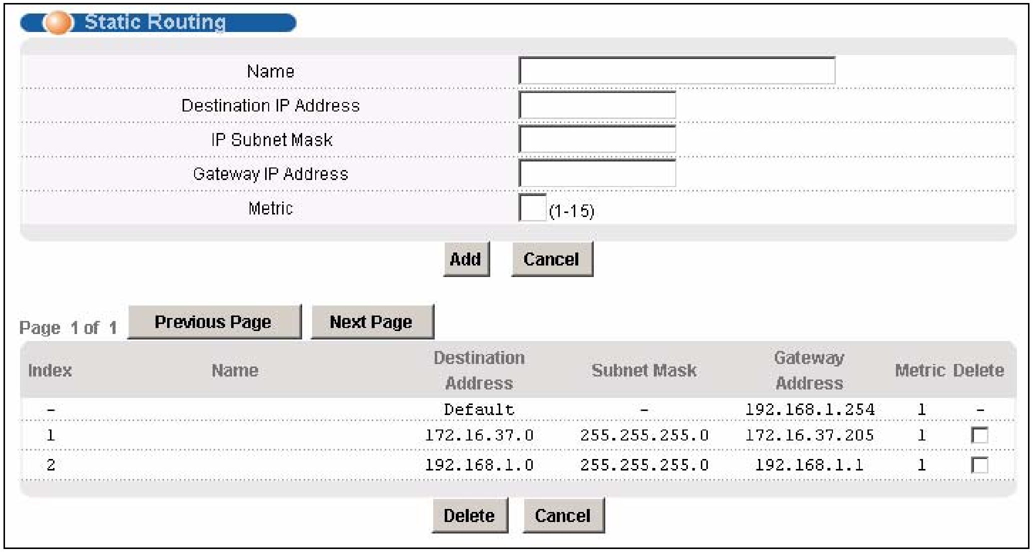
Static Routing

This chapter shows you how to configure the static routing function.

Static routes tell the IP DSLAM how to forward the IP DSLAM’s own IP traffic when you configure the TCP/IP parameters manually. This is generally useful for allowing management of the device from a device with an IP address on a different subnet from that of the device’s IP address (remote management).

To open this screen, click **Routing** > **Static Routing**.

Figure 138 Static Routing



Name	
Destination IP Address	
IP Subnet Mask	
Gateway IP Address	
Metric	(1-15)

Index	Name	Destination Address	Subnet Mask	Gateway Address	Metric	Delete
-		Default	-	192.168.1.254	1	-
1		172.16.37.0	255.255.255.0	172.16.37.205	1	□
2		192.168.1.0	255.255.255.0	192.168.1.1	1	□

The following table describes the labels in this screen.

Table 104 Static Routing

LABEL	DESCRIPTION
	Use this section to create a new static route.
Name	Type a name to identify this static route. Use up to 31 ASCII characters. Spaces and tabs are not allowed.
Destination IP Address	This parameter specifies the IP network address of the final destination. Routing is always based on network number. If you need to specify a route to a single host, use a subnet mask of 255.255.255.255 in the subnet mask field to force the network number to be identical to the host ID.
IP Subnet Mask	Enter the subnet mask for this destination.
Gateway IP Address	Enter the IP address of the gateway. The gateway is an immediate neighbor of your device that will forward the packet to the destination. The gateway must be a router on the same segment as your device.

Table 104 Static Routing (continued)

LABEL	DESCRIPTION
Metric	The metric represents the “cost” of transmission for routing purposes. IP routing uses hop count as the measurement of cost, with a minimum of 1 for directly connected networks. Enter a number that approximates the cost for this link. The number need not be precise, but it must be between 1 and 15. In practice, 2 or 3 is usually a good number.
Add	Click **Add** to save the new rule to the IP DSLAM’s volatile memory. It then displays in the summary table at the bottom of the screen. The IP DSLAM loses these changes if it is turned off or loses power, so use the **Config Save** link on the navigation panel to save your changes to the non-volatile memory when you are done configuring.
Cancel	Click **Cancel** to reset the fields to your previous configuration.
	Use this section to look at a summary of all static routes in the IP DSLAM.
Previous Page	Click this to display the preceding page of static route entries.
Next Page	Click this to display the following page of static route entries.
Index	This field displays the index number of the route.
Name	This field displays the name of this static route.
Destination Address	This field displays the IP network address of the final destination.
Subnet Mask	This field displays the subnet mask for this destination.
Gateway Address	This field displays the IP address of the gateway. The gateway is an immediate neighbor of your device that will forward the packet to the destination.
Metric	This field displays the cost of transmission for routing purposes.
Delete	Select the rule(s) that you want to remove in the **Delete** column, and then click the **Delete** button.
Cancel	Click **Cancel** to clear the selected check boxes in the **Delete** column.

48

Alarm

This chapter shows you how to display the alarms, sets the severity level of an alarm(s) and where the system is to send the alarm(s) and set port alarm severity level threshold settings.

48.1 Alarm

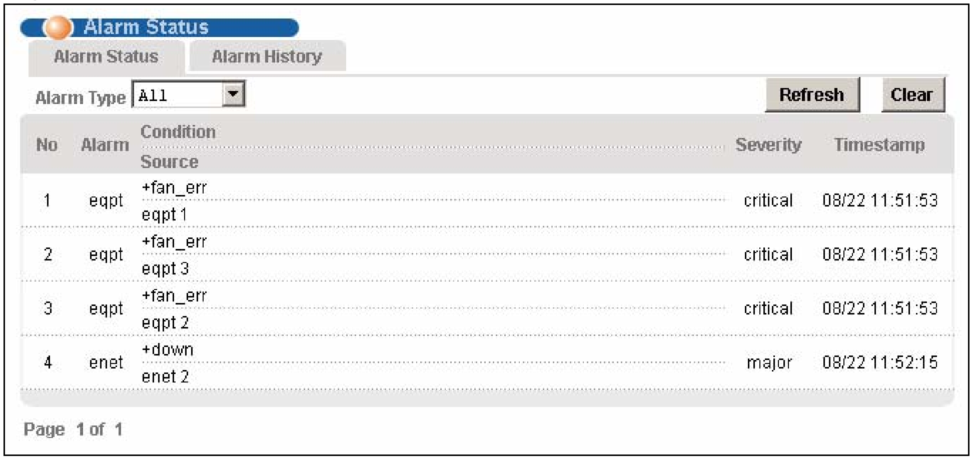
The IP DSLAM monitors for equipment, DSL and system alarms and can report them via SNMP or syslog. You can specify the severity level of an alarm(s) and where the system is to send the alarm(s). You can also set the alarm severity threshold for recording alarms on an individual port(s). The system reports an alarm on a port if the alarm has a severity equal to or higher than the port's threshold.

48.2 Alarm Status Screen

This screen displays the alarms that are currently in the system.

To open this screen, click **Alarm** > **Alarm Status**.

Figure 139 Alarm Status



Alarm Type: All

No	Alarm	Condition Source	Severity	Timestamp
1	eqpt	+fan_err eqpt 1	critical	08/22 11:51:53
2	eqpt	+fan_err eqpt 3	critical	08/22 11:51:53
3	eqpt	+fan_err eqpt 2	critical	08/22 11:51:53
4	enet	+down enet 2	major	08/22 11:52:15

Page 1 of 1

The following table describes the labels in this screen.

Table 105 Alarm Status

LABEL	DESCRIPTION
Alarm Type	Select which type of alarms to display by **Severity**, or select **All** to look at all the alarms.
Refresh	Click this button to update this screen.
Clear	Click this button to erase the clearable alarm entries.
No	This field displays the index number of the alarm entry in the system.
Alarm	This field displays the alarm category to which the alarm belongs.
Condition	This field displays a text description for the condition under which the alarm applies.
Severity	This field displays the alarm severity level (critical, major, minor or info).
Timestamp	This field displays the month, day, hour, minute and second that the system created the log.
Source	This field displays where the alarm originated. This is either a DSL port number, one of the Ethernet ports (enet 1 or 2), or “eqpt” for the system itself.
Page X of X	This identifies which page of information is displayed and the total number of pages of information.
Previous Page	Click this to display the preceding page of entries.
Next Page	Click this to display the following page of entries.

48.3 Alarm Descriptions

This table describes alarms that the system can send.

XTUC refers to the downstream channel (for traffic going from the IP DSLAM to the subscriber). XTUR refers to the upstream channel (for traffic coming from the subscriber to the IP DSLAM). A “V” in the **CLEARABLE** column indicates that an administrator can remove the alarm. You can use the CLI command “`alarm tablelist`” to display all alarm information on the IP DSLAM.

Table 106 Alarm Descriptions

ALARM	CONDITION	SEVERITY	CLEARABLE	DESCRIPTION
`dsl`	`(5000)line_up`	`info`	V	The DSL link is up.
`dsl`	`(5001)line_down`	`info`	V	The DSL link is down.
`dsl`	`(5002)vdsl_tca_lol`	`info`	V	The number of times a Loss Of Link has occurred within 15 minutes (for the XTUC) has reached the threshold.
`dsl`	`(5003)vdsl_tca_lof`	`info`	V	The number of times a Loss Of Frame has occurred within 15 minutes for the XTU (C or R) has reached the threshold.
`dsl`	`(5004)vdsl_tca_los`	`info`	V	The number of times a Loss Of Signal has occurred within 15 minutes for the XTU (C or R) has reached the threshold.

Table 106 Alarm Descriptions (continued)

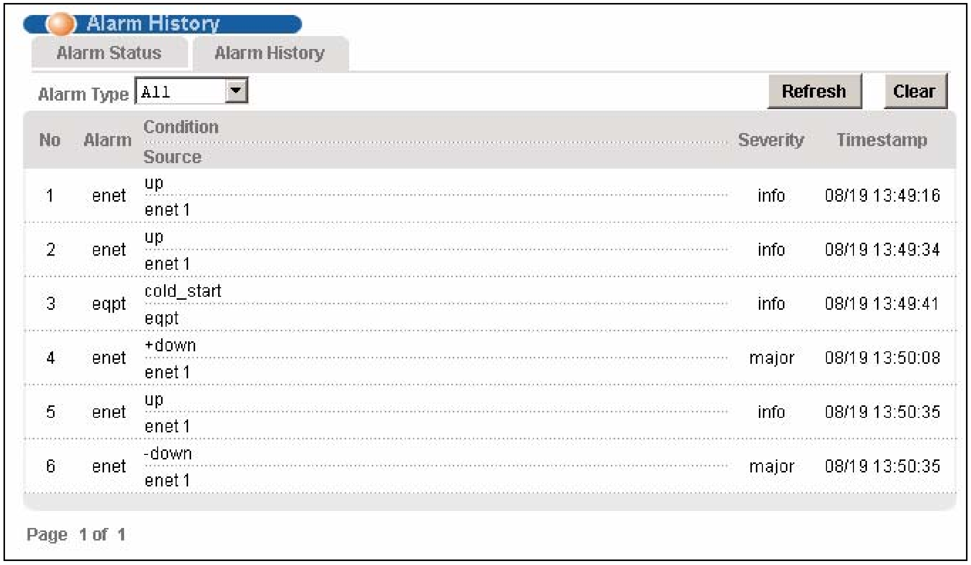
ALARM	CONDITION	SEVERITY	CLEARABLE	DESCRIPTION
dsl	(5005)vdsl_tca_lop	info	V	The number of times a Loss Of Power has occurred within 15 minutes for the XTU (C or R) has reached the threshold.
dsl	(5006)vdsl_tca_es	info	V	The number of error seconds within 15 minutes for the XTU (C or R) has reached the threshold.
dsl	(5007)vdsl_tca_ses	info	V	The number of severely errored seconds within 15 minutes for the XTU (C or R) has reached the threshold.
dsl	(5008)vdsl_tca_uas	info	V	The number of unavailable error seconds within 15 minutes for the XTU (C or R) has reached the threshold.
eqpt	(10000)vol_err	critical		The input voltage (Vn) is lower than the low-threshold or higher than the high-threshold.
eqpt	(10001)temp_err	critical		The temperature (Tn) is higher than the high-threshold or lower than the low-threshold.
eqpt	(10002)fan_err	critical		The fan RPM ‘n’ is over the high-threshold or lower than the low-threshold.
eqpt	(10003)hw_rtc_fail	critical		The Real Time Chip diagnosis test failed.
eqpt	(10004)hw_mon_fail	critical		The hardware monitor diagnosis test failed.
eqpt	(10005)cold_start	info		System cold-start.
eqpt	(10006)warm_start	info		System warm-start.
eqpt	(10007)alm_input	critical		There is an external alarm input.
sys	(15000)reboot	info		The system restarted.
sys	(15001)aco	info		An administrator cutoff (canceled) an alarm.
sys	(15002)alm_clear	info		An administrator cleared the alarms.
sys	(15003)login_fail	minor	V	Someone used the wrong name or password and failed to log in.
sys	(15004)anti_spoofing	minor	V	
enet	(20000)up	info		A Gigabit Ethernet interface is up.
enet	(20001)down	major	V	A Gigabit Ethernet interface is down.

48.4 Alarm History Screen

This screen displays the historical alarms stored in the system.

To open this screen, click **Alarm** > **Alarm History**.

Figure 140 Alarm History



Alarm Type All

No	Alarm	Condition Source	Severity	Timestamp
1	enet	up enet 1	info	08/19 13:49:16
2	enet	up enet 1	info	08/19 13:49:34
3	eqpt	cold_start eqpt	info	08/19 13:49:41
4	enet	+down enet 1	major	08/19 13:50:08
5	enet	up enet 1	info	08/19 13:50:35
6	enet	-down enet 1	major	08/19 13:50:35

Page 1 of 1

The following table describes the labels in this screen.

Table 107 Alarm History

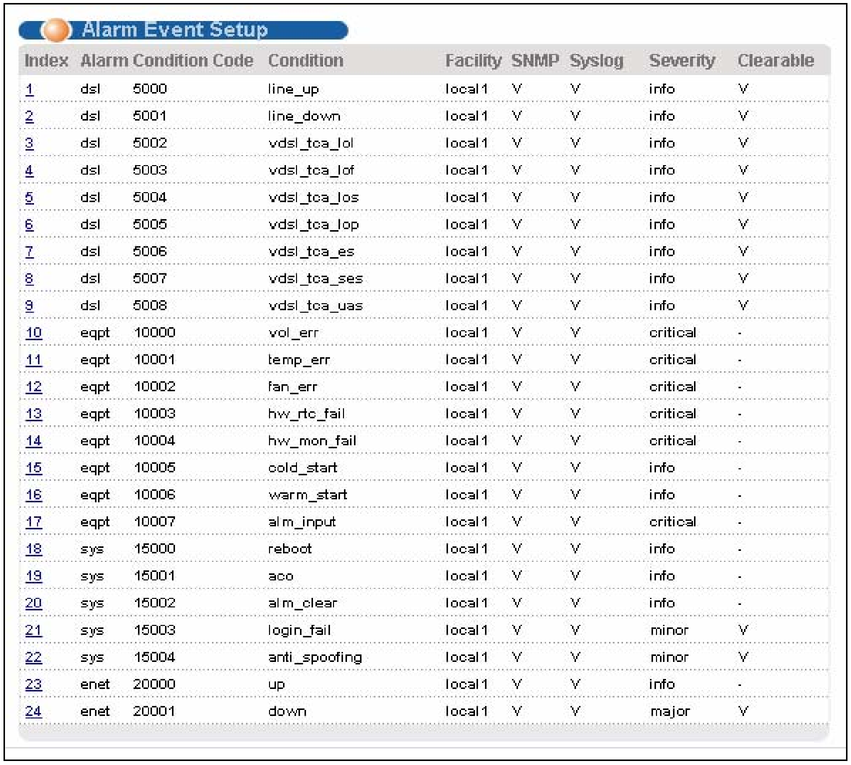
LABEL	DESCRIPTION
Alarm Type	Select which type of alarms to display by **Severity**, or select **All** to look at all the alarms.
Refresh	Click this button to update this screen.
Clear	Click this button to erase the clearable alarm entries.
No	This field displays the index number of the historial alarm entry in the system.
Alarm	This field displays the alarm category to which the alarm belongs.
Condition	This field displays a text description for the condition under which the historial alarm applies. See Section 48.3 on page 252 for alarm condition description.
Severity	This field displays the alarm severity level (critical, major, minor or info).
Timestamp	This field displays the month, day, hour, minute and second that the system created the log.
Source	This field displays where the alarm originated. This is either a DSL port number, one of the Ethernet ports (enet 1 or 2), or “eqpt” for the system itself.
Page X of X	This identifies which page of information is displayed and the total number of pages of information.
Previous Page	Click this to display the preceding page of entries.
Next Page	Click this to display the following page of entries.

48.5 Alarm Event Setup Screen

This screen lists the alarms that the system can generate along with the severity levels of the alarms and where the system is to send them.

To open this screen, click **Alarm** > **Alarm Event Setup**.

Figure 141 Alarm Event Setup



Alarm Event Setup

Index	Alarm	Condition Code	Condition	Facility	SNMP	Syslog	Severity	Clearable
1	dsl	5000	line_up	local1	V	V	info	V
2	dsl	5001	line_down	local1	V	V	info	V
3	dsl	5002	vdsl_tca_lol	local1	V	V	info	V
4	dsl	5003	vdsl_tca_lof	local1	V	V	info	V
5	dsl	5004	vdsl_tca_los	local1	V	V	info	V
6	dsl	5005	vdsl_tca_lop	local1	V	V	info	V
7	dsl	5006	vdsl_tca_es	local1	V	V	info	V
8	dsl	5007	vdsl_tca_ses	local1	V	V	info	V
9	dsl	5008	vdsl_tca_uas	local1	V	V	info	V
10	eqpt	10000	vol_err	local1	V	V	critical	-
11	eqpt	10001	temp_err	local1	V	V	critical	-
12	eqpt	10002	fan_err	local1	V	V	critical	-
13	eqpt	10003	hw_rtc_fail	local1	V	V	critical	-
14	eqpt	10004	hw_mon_fail	local1	V	V	critical	-
15	eqpt	10005	cold_start	local1	V	V	info	-
16	eqpt	10006	warm_start	local1	V	V	info	-
17	eqpt	10007	alm_input	local1	V	V	critical	-
18	sys	15000	reboot	local1	V	V	info	-
19	sys	15001	aco	local1	V	V	info	-
20	sys	15002	alm_clear	local1	V	V	info	-
21	sys	15003	login_fail	local1	V	V	minor	V
22	sys	15004	anti_spoofing	local1	V	V	minor	V
23	enet	20000	up	local1	V	V	info	-
24	enet	20001	down	local1	V	V	major	V

The following table describes the labels in this screen.

Table 108 Alarm Event Setup

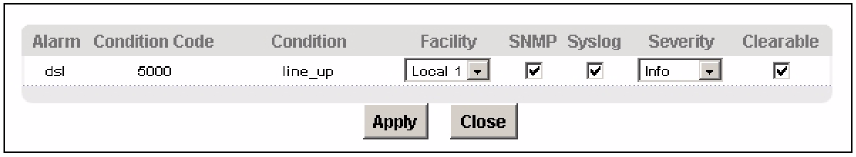
LABEL	DESCRIPTION
Index	This field displays the index number of the alarm in the list. Click this link to specify the severity level of an alarm(s) and where the system is to send the alarm(s). See Section 48.5.1 on page 256.
Alarm	This field displays the alarm category to which the alarm belongs. **dsl** represents Digital Subscriber Line (DSL) alarms. **enet** represents Ethernet alarms. **eqpt** represents equipment alarms. **sys** represents system alarms.
Condition Code	This field displays the condition code number for the specific alarm message.
Condition	This field displays a text description for the condition under which the alarm applies.
Facility	This field displays the log facility (Local 1~ Local 7) on the syslog server where the system is to log this alarm. This is for alarms that send alarms to a syslog server.
SNMP	This field displays “V” if the system is to send this alarm to an SNMP server. It displays “-“ if the system does not send this alarm to an SNMP server.
Syslog	This field displays “V” if the system is to send this alarm to a syslog server. It displays “-“ if the system does not send this alarm to a syslog server.
Severity	This field displays the alarm severity level (critical, major, minor or info).
Clearable	This displays “V” if the alarm clear command removes the alarm from the system. It displays “-“if the alarm clear command does not remove the alarm from the system.

48.5.1 Edit Alarm Event Setup Screen

Use this screen to specify the severity level of an alarm(s) and where the system is to send the alarm(s).

To open this screen, click **Alarm** > **Alarm Status**. Then, click an alarm's index number.

Figure 142 Alarm Event Setup Edit



Alarm	Condition Code	Condition	Facility	SNMP	Syslog	Severity	Clearable
dsl	5000	line_up	Local 1	☑	☑	Info	☑

The following table describes the labels in this screen.

Table 109 Alarm Event Setup Edit

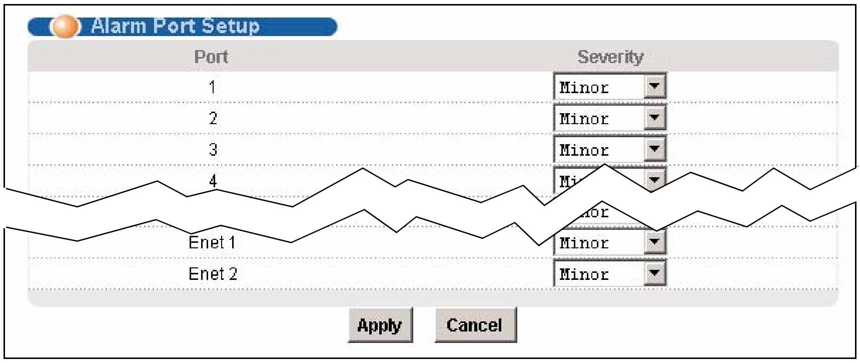
LABEL	DESCRIPTION
Alarm	This field displays the alarm category to which the alarm belongs. **eqpt** represents equipment alarms. **dsl** represents Digital Subscriber Line (DSL) alarms. **enet** represents Ethernet alarms. **sys** represents system alarms.
Condition Code	This field displays the condition code number for the specific alarm message.
Condition	This field displays a text description for the condition under which the alarm applies.
Facility	The log facility (Local 1 ~ Local 7) has the device log the syslog messages to a particular file in the syslog server. Select a log facility (Local 1 ~ Local 7) from the drop-down list box if this entry is for sending alarms to a syslog server. See your syslog program's documentation for details.
SNMP	Select this check box to have the system send this alarm to an SNMP server.
Syslog	Select this check box to have the system send this alarm to a syslog server.
Severity	Select an alarm severity level (critical, major, minor or info) for this alarm. Critical alarms are the most severe, major alarms are the second most severe, minor alarms are the third most severe and info alarms are the least severe.
Clearable	Select this check box to allow administrators to use the management interface to remove an alarm report generated by this alarm event entry. Select this check box to keep an alarm report generated by this alarm event in the system until the conditions that caused the alarm report are no longer present.
Apply	Click **Apply** to save your changes to the IP DSLAM's volatile memory. The IP DSLAM loses these changes if it is turned off or loses power, so use the **Config Save** link on the navigation panel to save your changes to the non-volatile memory when you are done configuring.
Close	Click **Close** to exit the screen without saving your changes.

48.6 Alarm Port Setup Screen

Use this screen to set the alarm severity threshold for recording alarms on an individual port(s). The system reports an alarm on a port if the alarm has a severity equal to or higher than the port's threshold.

To open this screen, click **Alarm** > **Alarm Port Setup**.

Figure 143 Alarm Port Setup



The following table describes the labels in this screen.

Table 110 Alarm Port Setup

LABEL	DESCRIPTION
Port	This column lists the device’s individual DSL and Ethernet interfaces.
Severity	Select an alarm severity level (critical, major, minor or info) as the threshold for recording alarms on this port. Critical alarms are the most severe, major alarms are the second most severe, minor alarms are the third most severe and info alarms are the least severe.
Apply	Click **Apply** to save your changes to the IP DSLAM’s volatile memory. The IP DSLAM loses these changes if it is turned off or loses power, so use the **Config Save** link on the navigation panel to save your changes to the non-volatile memory when you are done configuring.
Cancel	Click **Cancel** to start configuring the screen again.

49

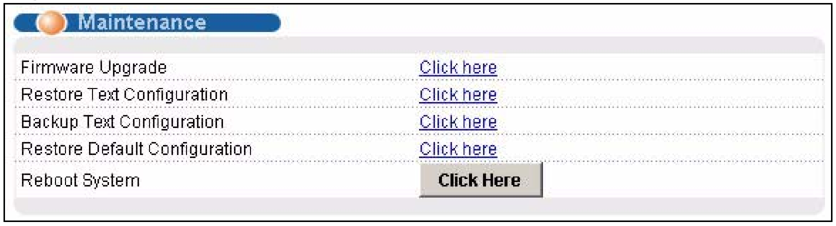
Maintenance

This chapter explains how to use the maintenance screens.

49.1 Maintenance Screen

To open this screen, click **Management** > **Maintenance**.

Figure 144 Maintenance



Maintenance

Firmware Upgrade	Click here
Restore Text Configuration	Click here
Backup Text Configuration	Click here
Restore Default Configuration	Click here
Reboot System	Click Here

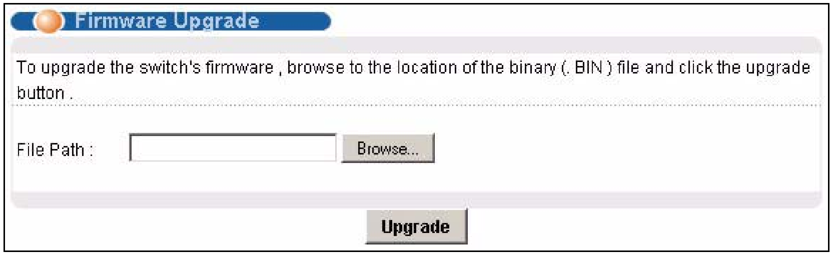
49.2 Firmware Upgrade Screen

Use this screen to upgrade your device firmware. See the **System Info** screen to verify your current firmware version number. Make sure you have downloaded (and unzipped) the correct model firmware and version to your computer before uploading to the device.

Be sure to upload the correct model firmware as uploading the wrong model firmware may damage your device.

To open this screen, click **Management** > **Maintenance** > **Firmware Upgrade**.

Figure 145 Firmware Upgrade



Firmware Upgrade

To upgrade the switch's firmware , browse to the location of the binary (. BIN) file and click the upgrade button .

File Path :

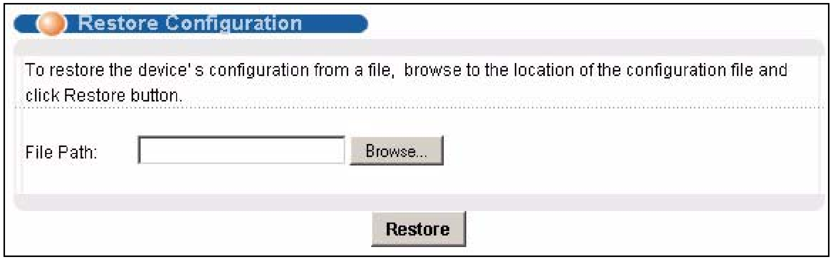
Type the path and file name of the firmware file you wish to upload to the device in the **File Path** text box or click **Browse** to locate it. After you have specified the file, click **Upgrade**.

49.3 Restore Configuration Screen

Use this screen to load a configuration file from your computer to the device.

To open this screen, click **Management > Maintenance** > **Restore Text Configuration**.

Figure 146 Restore Configuration



Restore Configuration

To restore the device' s configuration from a file, browse to the location of the configuration file and click Restore button.

File Path:

Type the path and file name of the configuration file you wish to restore in the **File Path** text box or click **Browse** to display a **Choose File** screen from which you can locate it. After you have specified the file, click **Restore**. "conf-0" is the name of the configuration file on the device, so your backup configuration file is automatically renamed when you restore using this screen.

If you load an invalid configuration file, it may corrupt the settings, and you might have to use the console to reconfigure the system.

49.4 Backing Up a Configuration File

Backing up your device configurations allows you to create various “snap shots” of your device from which you may restore at a later date.

Click **Management > Maintenance** > **Backup Text Configuration**. In the prompted **File Download** screen, click **Save** and choose a location to save the file on your computer from the **Save in** drop-down list box and type a descriptive name for it in the **File name** list box. Click **Save** to save the configuration file to your computer.

See the chapters on commands to edit the configuration text file.

You can change the “.dat” file to a “.txt” file and still upload it back to the IP DSLAM.

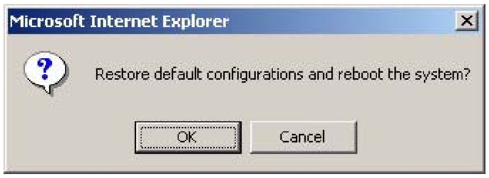
49.5 Load Factory Defaults

Use this function to clear all device configuration information you configured and return to the factory defaults.

Restoring the default configuration deletes all the current settings. It is recommended to back up the configuration file before restoring the default configuration.

To do this, click **Management** > **Maintenance** > **Restore Default Configuration**.

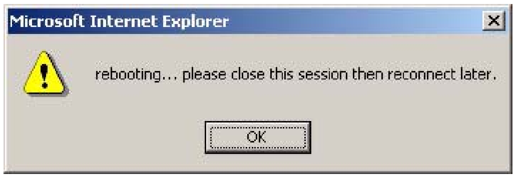
Figure 147 Restore Default Configuration



Restore default configurations and reboot the system?

Click **OK** to begin resetting all device configurations to the factory defaults and then wait for the device to restart. This takes up to two minutes. If you want to access the device web configurator again, you may need to change the IP address of your computer to be in the same subnet as that of the default device IP address (192.168.1.1).

Figure 148 Restore Factory Default Settings, Reboot



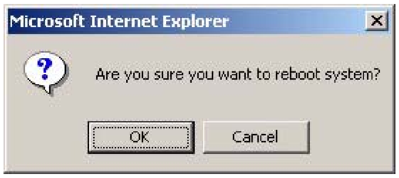
rebooting... please close this session then reconnect later.

49.6 Reboot System

Use this function to restart the device without physically turning the power off.

To open this screen, click **Management > Maintenance** > **Click here** (Reboot System).

Figure 149   Reboot System



Microsoft Internet Explorer

Are you sure you want to reboot system?

Click **OK**. You then see the screen as shown in Figure 148 on page 261. Click **OK** again and wait for the device to restart. This takes up to two minutes. This does not affect the device’s configuration.

49.7 Command Line FTP

See the VES DSLAM CLI Reference Guide for how to upload or download files to or from the device using FTP commands.

50

Diagnostics

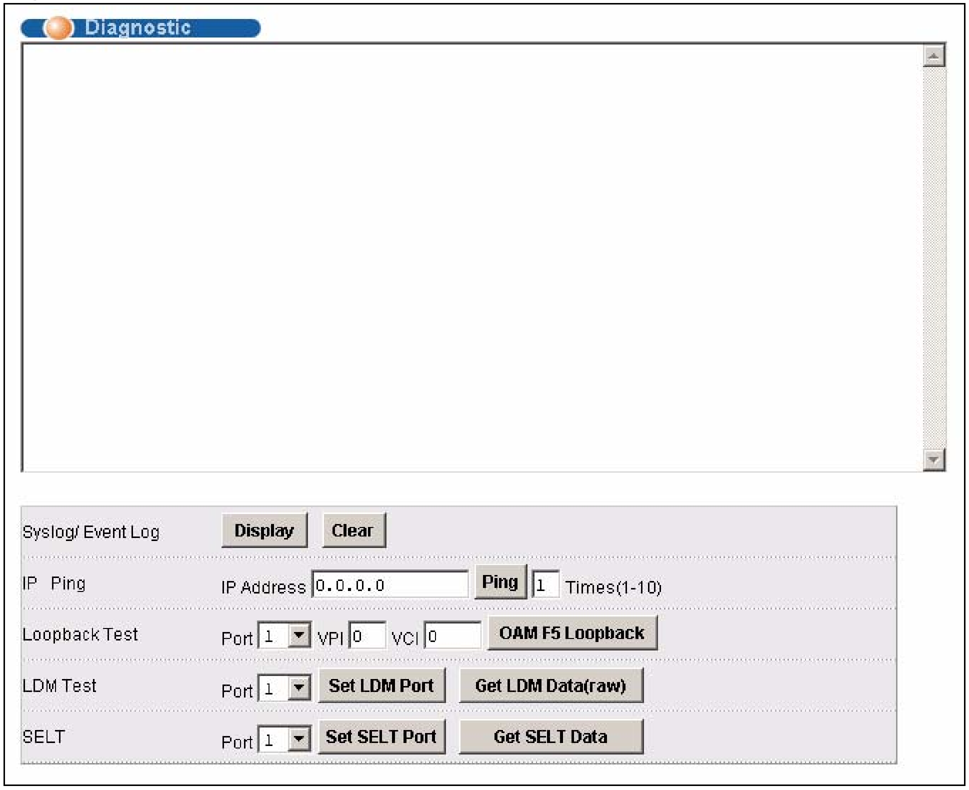
This chapter explains the Diagnostic screens.

50.1 Diagnostics Screen

Use this screen to check system logs, ping IP addresses or perform loopback tests.

To open this screen, click **Management** > **Diagnostic**.

Figure 150 Diagnostic



Syslog/ Event Log	Display	Clear		
IP Ping	IP Address 0.0.0.0	Ping	1 Times(1-10)	
Loopback Test	Port 1	VPI 0	VCI 0	OAM F5 Loopback
LDM Test	Port 1	Set LDM Port	Get LDM Data(raw)	
SELT	Port 1	Set SELT Port	Get SELT Data	

The following table describes the labels in this screen.

Table 111 Diagnostics

LABEL	DESCRIPTION
Syslog/ Event Log	Click **Display** to display a log of events in the multi-line text box. Click **Clear** to empty the text box and reset the log.
IP Ping	Type the **IP Address** of a device that you want to ping in order to test a connection. In the **Times** field specify how often you want to ping the IP address. Select the **Interface** from which you want to ping the IP address (**Ethernet**). Click **Ping** to have the device ping the IP address (in the field to the left).
Loopback Test	Select a port number from the **Port** drop-down list box and enter a VPI/VCI to specify a PVC. Click **OAM F5 Loopback** to perform an OAMF5 loopback test on the specified DSL port. An Operational, Administration and Maintenance Function 5 test is used to test the connection between two DSL devices. First, the DSL devices establish a virtual circuit. Then the local device sends an ATM F5 cell to be returned by the remote DSL device (both DSL devices must support ATM F5 in order to use this test). The results ("Passed" or "Failed") display in the multi-line text box.
LDM Test	Select a port number from the **Port** drop-down list box and click **Set LDM Port** to have the IP DSLAM perform line diagnostics on the specified port. The xDSL port must have a connection. It takes about one minute for the line diagnostics to finish. The screen displays a message confirming upon which DSL port line diagnostics will be performed. Click **Get LDM Data** to display the line diagnostics results after using the **Set LDM Port** button on an DSL port. Use the line diagnostics results to analyze problems with the physical xDSL line. Click **Get LDM Data(raw)** to display the unformatted line diagnostics results. Click **Get LDM Data(992.3)** to display the line diagnostics results in the format defined in the ITU-T G.992.3 standard. Note: Wait at least one minute after using Set LDM Port before using Get LDM Data.
SELT	Select a port number from the **Port** drop-down list box and click **Set SELT Port** to perform a Single End Loop Test (SELT) on the specified port. This test checks the distance to the subscriber's location. Note: The port must have an open loop. There cannot be a DSL device, phone, fax machine or other device connected to the subscriber's end of the telephone line. The SELT takes at least fifteen seconds. To check the status of the SELT or to look at the results when the SELT is complete, select a port number from the **Port** drop-down list box and click **Get SELT Data**. The results tell you what gauge of telephone wire is connected to the port and the approximate length of the line.

50.2 Log Format

The common format of the system logs is: `<item no> <time> <process> <type> <log message>`.

Table 112 Log Format

LABEL	DESCRIPTION
`<item no>`	This is the index number of the log entry.
`<time>`	This is the time and date when the log was created.
`<process>`	This is the process that created the log.
`<type>`	This identifies what kind of log it is. "INFO" identifies an information log. "WARN" identifies a warning log.
`<log message>`	This is the log's detailed information (see Table 113 on page 265).

50.2.1 Log Messages

The following table lists and describes the system log messages.

Table 113 Log Messages

LOG MESSAGE	TYPE	DESCRIPTION

`xDSL <port> Link Up(SN=<seq no>): <ds rate>/<us rate>!`
or
`xDSL Link Info: NM:<ds NM>/<us NM>!`
	INFO	A DSL port established a connection.
		<port> - port number
		<seq no> - sequence number of the connection
		<ds rate> - downstream rate
		<us rate> - upstream rate
		<us NM> - upstream noise margin
		<ds NM> - downstream noise margin

`xDSL <port> Link Down(SN=<seq no>)!`	WARN	A DSL port lost its connection. <port> - port number <seq no> - sequence number of the connection
`Session Begin!`	INFO	A console, telnet or FTP session has begun (see the <process> field for the type of session).
`Session End!`	INFO	A console telnet or FTP session has terminated (see the <process> field for the type of session).
`Incorrect Password!`	WARN	Someone attempted to use the wrong password to start a console, telnet or FTP session (see the <process> field for the type of session).
`Received Firmware Checksum Error!`	WARN	A checksum error was detected during an attempted FTP firmware upload.
`Received Firmware Size too large!`	WARN	The file size was too large with an attempted FTP firmware upload.
`Received Firmware Invalid!`	WARN	Someone attempted to upload a firmware file with a wrong identity via FTP.
`Received File <file>!`	INFO	A file was uploaded to the IP DSLAM by FTP. <file> - received file's name

Table 113 Log Messages (continued)

LOG MESSAGE	TYPE	DESCRIPTION
`THERMO OVER TEMPERATURE: dev:<id> threshold:<threshold> (degree C) value:<temp>(degree C)!`	`WARN`	The temperature was too high at one of the temperature sensors. <id> - 0: sensor near the DSL chipset 1: sensor near the CPU 2: thermal sensor chip itself <threshold> - threshold temperature <temp> - temperature when the entry was logged
`THERMO OVER TEMPERATURE released: dev:<id> threshold:<threshold> (degree C) value:<temp>(degree C)!`	`INFO`	The temperature at one of the temperature sensors has come back to normal. <id> 0: sensor near the DSL chipset 1: sensor near the CPU 2: thermal sensor chip itself <threshold> - threshold temperature <temp> - temperature when the entry was logged
`THERMO OVER VOLTAGE: nominal:<nominal>(mV) value:<voltage> mV)!`	`WARN`	The voltage went outside of the accepted operating range. <nominal> - nominal voltage of the DC power <voltage> - voltage of the DC power when logged
`THERMO OVER VOLTAGE released: nominal:<nominal>(mV) value:<voltage> (mV)!`	`INFO`	The voltage is back inside the accepted operating range. <nominal> - nominal voltage of the DC power <voltage> - voltage of the DC power when logged

50.3 LDM Test Parameters

The following table lists the line diagnostics test parameters that display, see the ITU-T’s G.992.3 for more information.

Table 114 LDM Test Parameters

LABEL	DESCRIPTION
`number_of_ subcarries`	Discrete Multi-Tone (DMT) modulation divides up a line’s bandwidth into sub-carriers (sub-channels) of 4.3125 KHz each. The first number is the total number of DMT sub-carriers the DSL connection is using. The second number indicates how many upstream DMT sub-carriers the DSL connection is using.
`hlinScale:`	The channel characteristics function is represented in linear format by a scale factor and a complex number. These are the maximum upstream and downstream scale factors used in producing the channel characteristics function.
`latn:`	This is the upstream and downstream Line Attenuation (in dB).
`satn:`	This is the upstream and downstream Signal Attenuation (in dB).
`snrm:`	This is the upstream and downstream Signal-to-Noise Ratio Margin (in dB). A DMT sub-carrier’s SNR is the ratio between the received signal power and the received noise power. The signal-to-noise ratio margin is the maximum that the received noise power could increase with the IP DSLAM still being able to meet its transmission targets.
`attndr:`	This is the upstream and downstream Attainable Net Data Rate (in bit/s).

Table 114 LDM Test Parameters (continued)

LABEL	DESCRIPTION
`farEndActatp:`	This is the upstream and downstream Far End Actual Aggregate Transmit Power (in dBm)
`i`	This is the index number of the DMT sub-carrier.
`li.rl`	The channel characteristics function is represented in linear format by a scale factor and a complex number. This is the real part of the complex number used in producing the channel characteristics function for this sub-carrier.
`li.im`	The channel characteristics function is represented in linear format by a scale factor and a complex number. This is the imaginary part of the complex number used in producing the channel characteristics function for this sub-carrier
`log`	This is a format for providing channel characteristics. It provides magnitude values in a logarithmic scale. This can be used in analyzing the physical condition of the DSL line.
`QLN`	The Quiet Line Noise for a DMT sub-carrier is the rms (root mean square) level of the noise present on the line, when no DSL signals are present. It is measured in dBm/Hz. The QLN can be used in analyzing crosstalk.
`SNR`	This is the upstream and downstream Signal-to-Noise Ratio (in dB). A DMT sub-carrier's SNR is the ratio between the received signal power and the received noise power. The SNR can be used in analyzing time dependent changes in crosstalk levels and line attenuation (such as those caused by temperature variations and moisture).

50.4 ToneDiag Parameters

The following table lists the tone diagnostic parameters that display, see the ITU-T's G.992.3 for more information.

Table 115 ToneDiag Parameters

LABEL	DESCRIPTION
`number_of_ subcarries`	Discrete Multi-Tone (DMT) modulation divides up a line's bandwidth into sub-carriers (sub-channels) of 4.3125 KHz each. This number indicates how many upstream and downstream DMT sub-carriers the DSL connection is using.
`hlinScale:`	The channel characteristics function is represented in linear format by a scale factor and a complex number. This is the maximum upstream and downstream scale factor used in producing the channel characteristics function.
`latn:`	This is the upstream and downstream Line Attenuation (in dB).
`satn:`	This is the upstream and downstream Signal Attenuation (in dB).
`snrm:`	This is the upstream and downstream Signal-to-Noise Ratio Margin (in dB). A DMT sub-carrier's SNR is the ratio between the received signal power and the received noise power. The signal-to-noise ratio margin is the maximum that the received noise power could increase with the IP DSLAM still being able to meet its transmission targets.
`attndr:`	This is the upstream and downstream Attainable Net Data Rate (in bit/s).
`farEndActatp:`	This is the upstream and downstream Far End Actual Aggregate Transmit Power (in dBm)
`i`	This is the index number of the DMT sub-carrier.

Table 115 ToneDiag Parameters (continued)

LABEL	DESCRIPTION
`logdB)`	This is a format for providing channel characteristics. It provides magnitude values in a logarithmic scale. This can be used in analyzing the physical condition of the DSL line.
`QLN(dBm)`	The Quiet Line Noise for a DMT sub-carrier is the rms (root mean square) level of the noise present on the line, when no DSL signals are present. It is measured in dBm/Hz. The QLN can be used in analyzing crosstalk.
`SNR(dB)`	This is the upstream and downstream Signal-to-Noise Ratio (in dB). A DMT sub-carrier’s SNR is the ratio between the received signal power and the received noise power. The SNR can be used in analyzing time dependent changes in crosstalk levels and line attenuation (such as those caused by temperature variations and moisture).

51

MAC Table

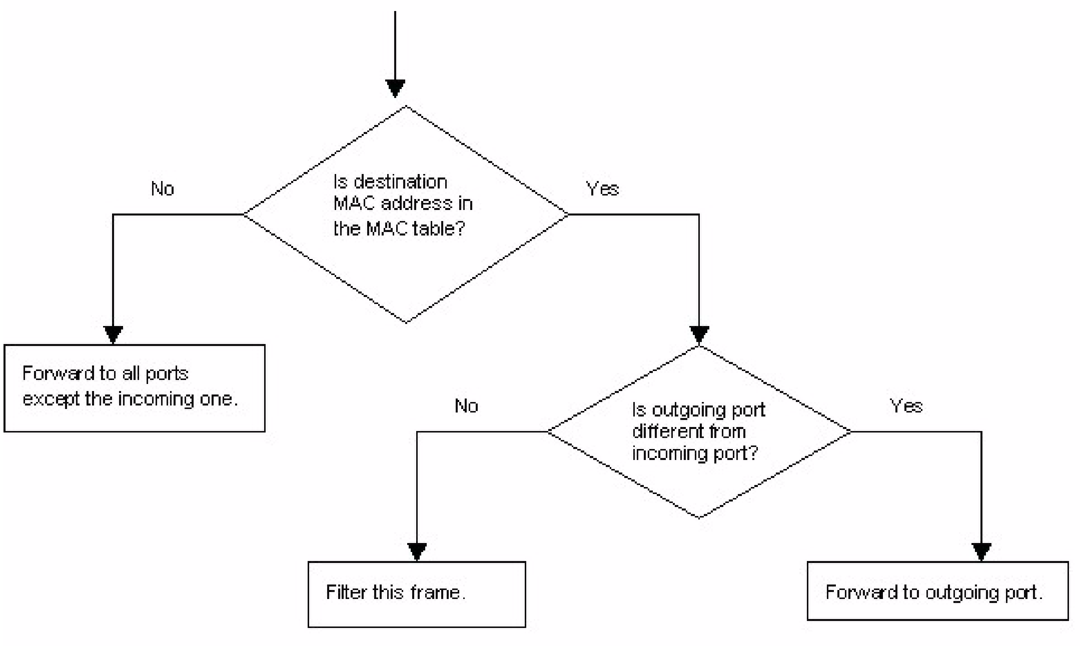
This chapter introduces the MAC Table.

51.1 Introduction to MAC Table

The MAC table lists device MAC addresses that are dynamically learned by the IP DSLAM. The table shows the following for each MAC address: the port upon which Ethernet frames were received from the device, to which VLAN groups the device belongs (if any) and to which channel it is connected (for devices connected to DSL ports).

The device uses the MAC table to determine how to forward frames. See the following figure.

Figure 151 MAC Table Filtering Flowchart


Is destination MAC address in the MAC table?
No
Yes
Forward to all ports except the incoming one.
Is outgoing port different from incoming port?
No
Yes
Filter this frame.
Forward to outgoing port.

1 The device examines a received frame and learns the port on which this source MAC address came.

2 The device checks to see if the frame's destination MAC address matches a source MAC address already learned in the MAC table.

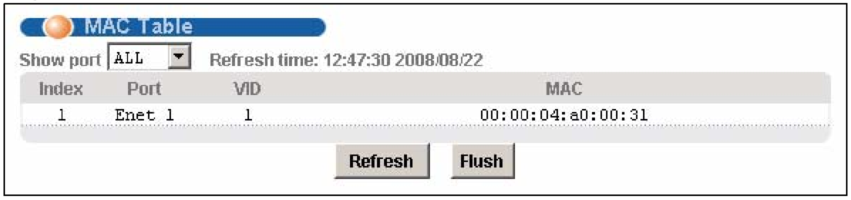
- If the device has already learned the port for this MAC address, then it forwards the frame to that port.

- If the device has not already learned the port for this MAC address, then the frame is flooded to all ports. Too much port flooding leads to network congestion.
- If the device has already learned the port for this MAC address, but the destination port is the same as the port it came in on, then it filters the frame.

51.2 MAC Table Screen

To open this screen, click **Management** > **MAC Table**.

Figure 152 MAC Table



Show port: ALL

Refresh time: 12:47:30 2008/08/22

Index	Port	VID	MAC
1	Enet 1	1	00:00:04:a0:00:31

The following table describes the labels in this screen.

Table 116 MAC Table

LABEL	DESCRIPTION
Show port	Select a port for which to display learned MAC addresses (or display all of them).
Page X of X	This identifies which page of information is displayed and the total number of pages of information.
Previous/Next	Click one of these buttons to show the previous/next screen if all of the information cannot be seen in one screen.
Index	This is the number of the MAC table entry.
Port	This is the port to which the MAC address is associated.
VID	This is the VLAN identifier of the MAC table entry.
MAC	This is the MAC address of the device from which this incoming frame came.
Refresh	Click **Refresh** to update the list of dynamically learned MAC addresses.
Flush	Click **Flush** to remove all of the dynamically learned MAC address entries from the MAC table.

52

ARP Table

This chapter describes the ARP Table.

52.1 Introduction to ARP Table

Address Resolution Protocol (ARP) is a protocol for mapping an Internet Protocol address (IP address) to a physical machine address, also known as a Media Access Control or MAC address, on the local area network.

An IP (version 4) address is 32 bits long. In an Ethernet LAN, MAC addresses are 48 bits long. The ARP Table maintains an association between each MAC address and its corresponding IP address.

52.1.1 How ARP Works

When an incoming packet destined for a host device on a local area network arrives at the device, the device's ARP program looks in the ARP Table and, if it finds the address, sends it to the device.

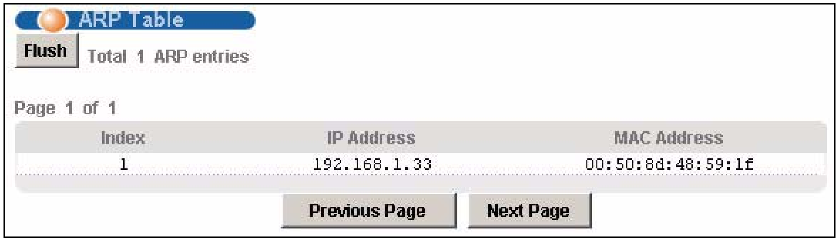
If no entry is found for the IP address, ARP broadcasts the request to all the devices on the LAN. The device fills in its own MAC and IP address in the sender address fields, and puts the known IP address of the target in the target IP address field. In addition, the device puts all ones in the target MAC field (FF.FF.FF.FF.FF.FF is the Ethernet broadcast address). The replying device (which is either the IP address of the device being sought or the router that knows the way) replaces the broadcast address with the target's MAC address, swaps the sender and target pairs, and unicasts the answer directly back to the requesting machine. ARP updates the ARP Table for future reference and then sends the packet to the MAC address that replied.

52.2 ARP Table Screen

The ARP table can hold up to 500 entries.

To open this screen, click **Management** > **ARP Table**.

Figure 153 ARP Table



Total 1 ARP entries

Page 1 of 1

Index	IP Address	MAC Address
1	192.168.1.33	00:50:8d:48:59:1f

The following table describes the labels in this screen.

Table 117 ARP Table

LABEL	DESCRIPTION
Flush	Click **Flush** to remove all of the entries from the ARP table.
Total X ARP Entries	This displays the number of entries in the ARP table.
Page X of X	This identifies which page of information is displayed and the total number of pages of information.
Index	This is the ARP table entry number.
IP Address	This is the learned IP address of a device connected to a port.
MAC Address	This is the MAC address of the device with the listed IP address.
Previous Page Next Page	Click one of these buttons to show the preceding or following screen if the information cannot be displayed in one screen.

PART V

Troubleshooting and Specifications

53

Troubleshooting

This chapter covers potential problems and possible remedies. After each problem description, some steps are provided to help you to diagnose and solve the problem.

53.1 The SYS or PWR LED Does Not Turn On

The SYS/PWR LED does not turn on.

Table 118 SYS LED Troubleshooting

STEP	CORRECTIVE ACTION
1	Make sure the power wires are properly connected to the power supply and the power supply is operating normally. Make sure you are using the correct power source (see Chapter 54 on page 283).
2	Make sure the power wires are connected properly.
3	Make sure a fuse is not burnt-out. Replace a fuse if it is burnt-out. See Appendix A on page 291 for instructions.
4	The LED itself or the unit may be faulty; contact your vendor.

53.2 The ALM LED Is On

The **ALM** (alarm) LED lights when the IP DSLAM is overheated, the fans are not working properly, the voltage readings are outside the tolerance levels or an alarm has been detected on the ALARM input pins.

Table 119 ALM LED Troubleshooting

STEP	CORRECTIVE ACTION
1	Use the statistics monitor command to verify the cause of the alarm. See step 2 if the unit is overheated, step 3 if the problem is with the fans and step 4 if the voltages are out of the allowed ranges.
2	Ensure that the IP DSLAM is installed in a well-ventilated area and that normal operation of the fans is not inhibited. Keep the bottom, top and all sides clear of obstructions and away from the exhaust of other equipment.
3	Make sure you can feel and/or hear the fans working - working fans emit a low buzz and blow air.
4	If the voltage levels are outside the allowed range, take a screen shot of the statistics monitor command display and contact your vendor.

53.3 SFP LNK LEDs Do Not Turn On

The LEDs for one of the SFP slots do not turn on.

Table 120 SFP LNK LED Troubleshooting

STEPS	CORRECTIVE ACTION
1	Make sure that the Ethernet port's mode is set to match that of the peer Ethernet device.
2	Check the cable and connections between the SFP slot and the peer Ethernet device.
3	Check the mini GBIC transceiver.
4	Make sure that the peer Ethernet device is functioning properly. If the cable, transceiver and peer Ethernet device are all OK and the LEDs stay off, there may be a problem with the SFP slot. Contact the distributor.

53.4 100/1000 LEDs Do Not Turn On

A 100/1000 Ethernet port's LEDs do not turn on.

Table 121 100/1000 LED Troubleshooting

STEPS	CORRECTIVE ACTION
1	Each 100/1000M RJ-45 Ethernet port is paired with a mini GBIC slot. The IP DSLAM uses one connection per pair.
2	Check the **Speed Mode** settings in the **ENET Port Setup** screen. Make sure that the 100/1000 Ethernet port's connection speed is set to match that of the port on the peer Ethernet device. When an Ethernet port is set to **Auto**, the IP DSLAM tries to make a fiber connection first and does not attempt to use the RJ-45 port if the fiber connection is successful.
3	Check the Ethernet cable and connections between the 100/1000 Ethernet port and the peer Ethernet device. Use 1000Base-T 4-pair (8 wire) UTP Cat. 5 Ethernet cables with the RJ-45 interface.
4	Make sure that the peer Ethernet device is functioning properly. If the Ethernet cable and peer Ethernet device are both OK and the LEDs still stay off, there may be a problem with the port. Contact the distributor.

53.5 100/1000 Ethernet Port Data Transmission

The Ethernet port's LED is on, but data cannot be transmitted.

Table 122 Troubleshooting Data Transmission

STEPS	CORRECTIVE ACTION
1	Make sure that the Ethernet port has the appropriate mode setting.
2	Make sure that the IP DSLAM's IP settings are properly configured.
3	Check the VLAN configuration.
4	Ping the IP DSLAM from a computer behind the peer Ethernet device.

Table 122 Troubleshooting Data Transmission (continued)

STEPS	CORRECTIVE ACTION
5	If you cannot ping, check the Ethernet cable and connections between the Ethernet port and the Ethernet switch or router.
6	Check the switch mode. In daisychain mode, if you have a loop topology and enable RSTP, it is possible for RSTP to disable Ethernet port 1 (the uplink port). Note: It is not recommended to use daisychain mode in a loop topology.

53.6 DSL Data Transmission

The DSL link is up, but data cannot be transmitted.

Table 123 DSL Data Transmission Troubleshooting

STEPS	CORRECTIVE ACTION
1	Check the switch mode and port isolation settings. If an ADSL modem or router is connected to the port, check to see that the VPI/VCI and multiplexing mode (LLC/VC) settings in the subscriber’s DSL modem or router match those of the DSL port. If the subscriber is having problems with a video or other high-bandwidth services, make sure the IP DSLAM’s VDSL port’s data rates are set high enough.
2	Check the VLAN configuration.
3	Ping the IP DSLAM from the computer behind the VDSL modem or router.
4	If you cannot ping, connect a DSL modem to an VDSL port (that is known to work). If the VDSL modem or router works with a different VDSL port, there may be a problem with the original port. Contact the distributor.
5	If using a different port does not work, try a different VDSL modem or router with the original port.

53.7 There Is No Voice on an VDSL Connection

The IP DSLAM has internal POTS (Plain Old Telephone Service) splitters that allow the telephone wiring used for VDSL connections to also simultaneously carry normal voice conversations.

Table 124 VDSL Voice Troubleshooting

STEP	CORRECTIVE ACTION
1	Ensure that the subscriber’s VDSL is working normally.
2	Make sure the subscriber has a POTS splitter properly installed.
3	Check the VDSL line pin assignments shown in Chapter 54 on page 283.
4	Check the telephone wire connections between the subscriber and the MDF(s).
5	Check the telephone wire and connections between the MDF(s) and **VDSL** port(s).
6	Check the telephone wire mapping on the MDF(s).
7	Make sure the in-house wiring works and is connected properly.
8	Repeat the steps above using a different VDSL port.

53.8 Local Server

The computer behind a DSL modem or router cannot access a local server connected to the IP DSLAM.

Table 125 Troubleshooting a Local Server

STEPS	CORRECTIVE ACTION
1	See Section 53.6 on page 277 to make sure that the subscriber is able to transmit to the IP DSLAM.
2	Make sure the computer behind the DSL device has the correct gateway IP address configured.
3	Check the VLAN configuration (see Chapter 19 on page 133).
4	Check the cable and connections between the IP DSLAM and the local server.
5	Try to access another local server. If data can be transmitted to a different local server, the local server that could not be accessed may have a problem.

53.9 Data Rate

The SYNC-rate is not the same as the configured rate.

Table 126 Troubleshooting the SYNC-rate

STEPS	CORRECTIVE ACTION
1	Connect the VDSL modem or router directly to the VDSL port using a different telephone wire.
2	If the rates match, the quality of the telephone wiring that connects the subscriber to the VDSL port may be limiting the speed to a certain rate. If they do not match when a good wire is used, contact the distributor.

53.10 Configured Settings

The configured settings do not take effect.

Table 127 Troubleshooting the IP DSLAM’s Configured Settings

CORRECTIVE ACTION
Use the “config save” command after you finish configuring to save the IP DSLAM’s settings.

53.11 Password

If you forget your password, you will need to use the console port to reload the factory-default configuration file (see Section 53.15 on page 280).

53.12 System Lockout

Any of the following could also lock you and others out from using in-band management (managing through the data ports).

1. Deleting the management VLAN (default is VLAN 1).
2. Incorrectly configuring the CPU VLAN.
3. Incorrectly configuring the access control settings.
4. Disabling all ports.

Be careful not to lock yourself and others out of the system.

If you lock yourself (and others) out of the system, you can try using the console port to reconfigure the system. See Section 53.15 on page 280.

53.13 SNMP

The SNMP manager server cannot get information from the IP DSLAM.

Table 128 Troubleshooting the SNMP Server

STEPS	CORRECTIVE ACTION
1	Ping the IP DSLAM from the SNMP server. If you cannot, check the cable, connections and IP configuration.
2	Check to see that the community (or trusted host) in the IP DSLAM matches the SNMP server’s community.
3	Make sure that your computer’s IP address matches a configured trusted host IP address (if configured).

53.14 Telnet

I cannot telnet into the IP DSLAM.

Table 129 Troubleshooting Telnet

STEPS	CORRECTIVE ACTION
1	Make sure that the number maximum allowed number of telnet sessions has not already reached. The IP DSLAM only accepts up to five telnet sessions at a time. Make sure that a telnet session is not already operating. The IP DSLAM only accepts one telnet session at a time.
2	Make sure that your computer’s IP address matches a configured secured client IP address (if configured). The IP DSLAM immediately disconnects the telnet session if secured host IP addresses are configured and your computer’s IP address does not match one of them.

Table 129 Troubleshooting Telnet (continued)

STEPS	CORRECTIVE ACTION
3	Make sure that you have not disabled the Telnet service or changed the server port number that the IP DSLAM uses for Telnet.
5	Ping the IP DSLAM from your computer. If you are able to ping the IP DSLAM but are still unable to telnet, contact the distributor. If you cannot ping the IP DSLAM, check the cable, connections and IP configuration.

53.15 Resetting the Defaults

If you lock yourself (and others) from the IP DSLAM, you will need to reload the factory-default configuration file. Uploading the factory-default configuration file replaces the current configuration file with the factory-default configuration file. This means that you will lose all previous configurations and the speed of the console port will be reset to the default of 9600bps with 8 data bit, no parity, one stop bit and flow control set to none. The user name will be reset to “admin” and the password will be reset to “1234” and the IP address to 192.168.1.1.

53.15.1 Resetting the Defaults Via Command

If you know the password, you can reload the factory-default configuration file via Command Line Interface (CLI) command. Use the following procedure.

1. Connect to the console port using a computer with terminal emulation software. See chapters 2-6 for details.
2. Enter your password.
3. Type `config restore`.
4. Type `y` at the question “Do you want to restore default ROM file(y/n)?”
5. The IP DSLAM restarts.

Figure 154 Resetting the Switch Via Command

```
ras> config restore

System will reboot automatically after restoring default configuration.
Do you want to proceed(y/n)? >
restoring configuration...
saving configuration to flash...
```

The IP DSLAM is now reinitialized with a default configuration file including the default user name of “admin” and the default password of “1234”.

53.15.2 Uploading the Default Configuration File

If you forget your password or cannot access the IP DSLAM, you will need to reload the factory-default configuration file. Uploading the factory-default configuration file replaces the current configuration file with the factory-default configuration file. This means that you will lose all previous configurations and the speed of the console port will be reset to the default of 9600bps with 8 data bit, no parity, one stop bit and flow control set to none. The password will also be reset to “1234” and the IP address to 192.168.1.1.

Uploading the factory default configuration file erases the IP DSLAM’s entire configuration.

Obtain the default configuration file, unzip it and save it in a folder. Use a console cable to connect a computer with terminal emulation software to the IP DSLAM’s console port. Turn the IP DSLAM off and then on to begin a session. When you turn on the IP DSLAM again you will see the initial screen. When you see the message `Press any key to enter Debug Mode within 3 seconds` press any key to enter debug mode.

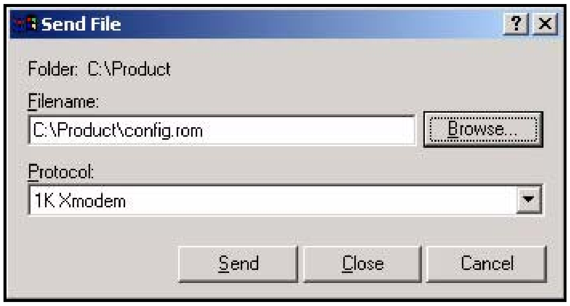
To upload the configuration file, do the following:

1 Type `atlc` after the `Enter Debug` Mode message.

2 Wait for the `Starting XMODEM upload` message before activating XMODEM upload on your terminal.

3 This is an example Xmodem configuration upload using HyperTerminal. Click **Transfer**, then **Send File** to display the following screen.

Figure 155 Example Xmodem Upload



Send File

Folder: C:\Product

Filename: C:\Product\config.rom

Protocol: 1K Xmodem

Type the configuration file's location, or click **Browse** to search for it. Choose the **1K Xmodem** protocol. Then click **Send**.

4 After a successful configuration file upload, type `atgo` to restart the IP DSLAM.

The IP DSLAM is now reinitialized with a default configuration file including the default password of “1234”.

53.16 Recovering the Firmware

Usually you should use FTP or the web configurator to upload the IP DSLAM's firmware. If the IP DSLAM will not start up, the firmware may be lost or corrupted. Use the following procedure to upload firmware to the IP DSLAM only when you are unable to upload firmware through FTP.

This procedure is for emergency situations only.

1 Obtain the firmware file, unzip it and save it in a folder on your computer.

2 Connect your computer to the console port and use terminal emulation software configured to the following parameters:

- VT100 terminal emulation
- 9600 bps
- No parity, 8 data bits, 1 stop bit
- No flow control

3 Turn off the IP DSLAM and turn it back on to restart it and begin a session.

4 When you see the message `Press any key to enter Debug Mode within 3 seconds`, press a key to enter debug mode.

5 Type `atba5` after the `Enter Debug Mode` message (this changes the console port speed to 115200 bps).

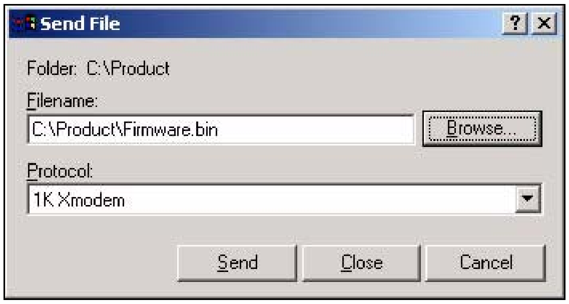
6 Change the configuration of your terminal emulation software to use 115200 bps and reconnect to the IP DSLAM.

7 Type `atur` after the `Enter Debug Mode` message.

8 Wait for the `Starting XMODEM upload` message before activating XMODEM upload on your terminal.

9 This is an example Xmodem configuration upload using HyperTerminal. Click **Transfer**, then **Send File** to display the following screen.

Figure 156 Example Xmodem Upload



Folder: C:\Product

Filename: C:\Product\Firmware.bin

Protocol: 1K Xmodem

Type the firmware file's location, or click **Browse** to search for it. Choose the **1K Xmodem** protocol. Then click **Send**.

10 After a successful firmware upload, type atgo to restart the IP DSLAM. The console port speed automatically changes back to 9600 bps when the IP DSLAM restarts.

54

Product Specifications

This chapter provides the specifications for the IP DSLAM.

54.1 Physical Specifications

The IP DSLAM is 19 inch (482.6 mm) rack-mountable.

Telco-50 Connectors

The IP DSLAM has 2 Telco-50 connectors. Connect the two VDSL Telco-50 connectors to the subscribers.

Dimensions

1.5 U 439.8 mm (W) x 251 mm (D) x 66 mm (H)

Weight

4.6 kg / 10.1 lbs

Wire Gauge Specifications

The following table shows the specifications for wire gauge.

Table 130 Wire Gauge Specifications

WIRE TYPE	REQUIRED AWG NO. (DIAMETER)
Ground Wire	18 or larger
Telephone Wire	26 or larger

AWG (American Wire Gauge) is a measurement system for wire that specifies its thickness. As the thickness of the wire increases, the AWG number decreases.

Power Input

100~240 VAC, 50/60 Hz, 1.3 A maximum

Power Consumption

64 W maximum

Fuse Rating

Changing the IP DSLAM’s fuses requires partial disassembly of the device. Only a qualified technician should perform this process.

The following table describes the location and specification of the IP DSLAM’s fuses.

Table 131 Fuse Specifications

FUSE LOCATION	FUSE RATING
On AC to DC power supply	250 VAC T4A 5*20

ALARM Port Power

The maximum power rating for the **ALARM** port is as follows:

- Input: 20 V, 500 mA
- Output: 20 V, 500 mA

Operating Environment

- Temperature: -10~60 °C
- Humidity: 10% ~ 95% (non-condensing)

Storage Environment

- Temperature: -40 ~ 70 °C
- Humidity: 5% ~ 95% (non-condensing)

Maximum Values

Per DSL port:

- Number of MAC filters: 10
- Number of OUI filters: 10
- Number of PVCs: 4Number of PVLAN: 8
- Number of VLANs: 16
- IGMP groups per DSL port: 16
- IGMP host IPs per DSL port: 16
- IGMP host IPs per Ethernet port: 1024
- Number of DHCP snooping: 32
- DHCP snooping static IP pool entries: 3
- Number of joined MVLANs: 4
- Number of ACL profile mappings: 8

System:

- Number of user accounts: 16
- Number of trap destinations: 4
- Number of secured client groups: 16

- Number of Telnet sessions: 5
- Number of VLANs: 1024
- Number of DSL profiles: 128
- Number of ATM profiles: 96
- Number of IGMP filter profiles: 128
- Number of IGMP proxy static query VLANs: 16
- Number of DSL alarm profiles: 8
- Number of Dot1X profiles: 64
- Number of DHCP relay servers: 32
- Number of IP routes: 128
- Number of static multicast addresses: 32
- Number of multicast group ranges per MVLAN: 16
- Number of multicast bandwidth control groups: 96
- Number of IGMP groups: 512 groups
- Number of learned MAC addresses: up to 4k entries
- Number of RPVC gateway IP addresses: 96
- Number of RPVC routing entries: 96
- Number of ACL profiles: 128
- Number of PPPoE Intermediate Agents: 48
- Number of VLAN Isolations: 16
- Number of MAC force forwarding entries: 64

54.2 Default Settings

This section lists the default configuration of the IP DSLAM.

Table 132 Default Settings

Default In-band IP Address	192.168.1.1
Default In-band Subnet Mask	255.255.255.0 (24 bits)
Default Out-of-band IP Address	192.168.0.1
Default Out-of-band Subnet Mask	255.255.255.0 (24 bits)
Default User Name	admin
Default Password	1234
Default Console Port Settings	VT100 terminal emulation, 9600 bps, No parity, 8 data bits, 1 stop bit, and no flow control
VLAN Default Settings	
VID	1
802.1p Priority	0
Registration	VLAN 1: Fixed for the Ethernet ports and VDSL ports
Tagging	Untagged for all ports
VDSL Default Settings	

Table 132 Default Settings (continued)

Name:	DEFVAL	
Latency Mode	Interleave	
	Upstream Settings:	Downstream Settings:
Maximum Rate	60000 kbps	100000 kbps
Minimum Rate	64 kbps	64 kbps
Interleave (latency) Delay	4 ms	4 ms
Maximum Margin	31 db	31 db
Minimum Margin	0 db	0 db
Target Margin	6 db	6 db
Upstream shift margin	9 db	9 db
Downstream shift margin	3 db	3 db
Rate Adaptation Mode	Startup	Startup
Ham Band Plan	0x0000	
Custom Notch1	Start: 0 (kHz)	Stop: 0 (kHz)
Custom Notch2	Start: 0 (kHz)	Stop: 0 (kHz)
VDSL2 Profile	6 (17a)	
Minimum Downstream INP	5 (0.5 DMT symbol)	
Minimum Upstream INP	5 (0.5 DMT symbol)	
Limit PSD Mask	2	
VDSL Option	0x00000000 enable us bitswaps enable ds bitswaps disable UPBO disable DPBO	
ESEL	0 (0.0 dB)	
UPBOESEL	0 (0.0 dB)	
DPBOEPSD	Break Point, Tone Index, (Frequency), PSD level 0, 1, (4.3125 kHz), -60.0 dBm 1, 32, (138.0 kHz), -60.0 dBm 2, 33, (142.3125 kHz), -40.0 dBm 3, 255, (1099.6875 kHz), -40.0 dBm 4, 376, (1595.6250 kHz), -50.0 dBm 5, 511, (2203.6875 kHz), -51.5 dBm 6, 512, (2208.0 kHz), -80.0 dBm	
DPBOESCMA	256 (scalar value: 0.0)	
DPBOESCMB	512 (scalar value: 1)	
DPBOESCMC	256 (scalar value: 0)	
DPBOMUS	180 (-90.0 dBm/Hz)	
DPBOFMIN	0 (0.0 kHz)	
DPBOFMAX	511 (2203.6875 kHz)	
UPBO Parameters	A	B
Upstream Band 1	5650 (56.50 dBm/Hz)	1019 (10.19 dBm/Hz)

Table 132 Default Settings (continued)

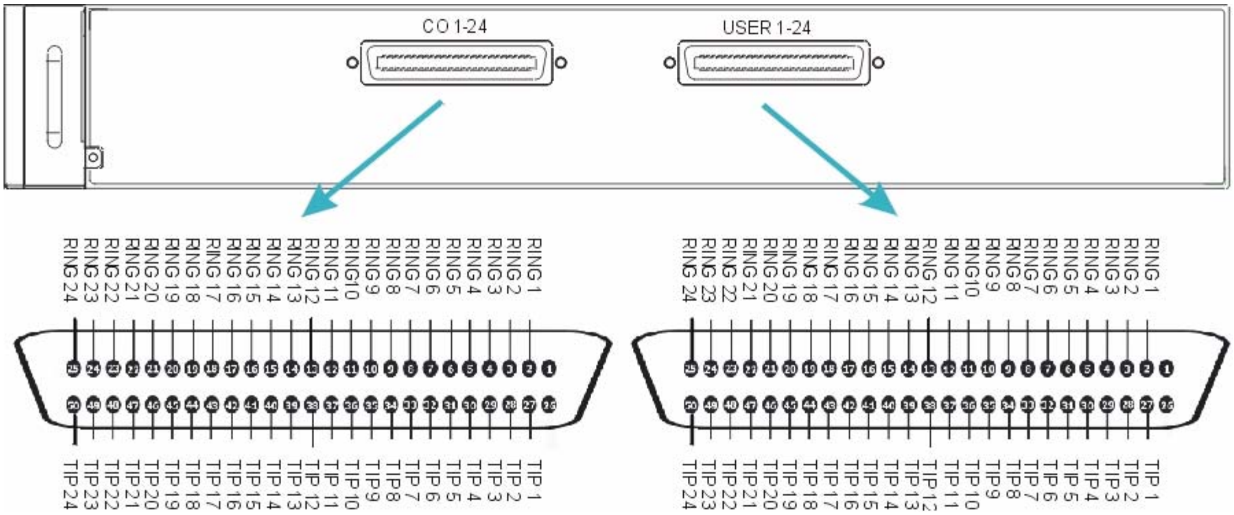
Upstream Band 2	5650 (56.50 dBm/Hz)	614 (6.14 dBm/Hz)
Upstream Band 3	0 (0.0 dBm/Hz)	0 (0.0 dBm/Hz)

54.3 Pin Assignments

54.3.1 Hardware Telco-50 Connector Pin Assignments

Connect to the IP DSLAM’s **CO 1-24** and **USER 1-24** ports using cables that have Telco-50 connectors with the following pin assignments.

Figure 157 CO 1-24 and USER 1-24 Telco-50 Pin Assignments



54.3.2 Console Cable Pin Assignments

The following diagrams and chart show the pin assignments of the console cable.

Figure 158 Console Cable RJ-11 Male Connector

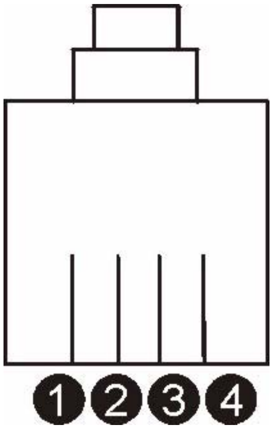


Figure 159 Console Cable DB-9 Female Connector

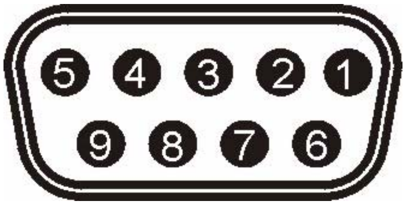


Table 133 Console Cable Connector Pin Assignments

RJ-11 MALE	DB-9 FEMALE
Pin 2: TXD	Pin 2
Pin 3: RXD	Pin 3
Pin 4: GND	Pin 5

54.4 ALARM Connector Pin Assignments

The following diagram shows the alarm connector pin layout.

Figure 160 ALARM Connector Pin Layout

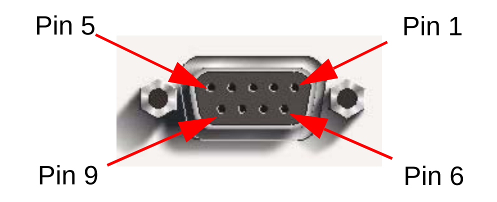


Table 134 ALARM Connector Pin Assignments

PIN	DESCRIPTION
1, 2, 6	Open the circuit of pins 1 and 6 and close the circuit of pins 2 and 6 to signal an alarm.
3, 7	Pins for alarm input 1.
4, 8	Pins for alarm input 2.
5, 8	Pins for alarm input 3.
9, 8	Pins for alarm input 4.

Alarm input is only for dry contact without any power. Open or short circuit is recommended.

PART VI
Appendices and Index

A

Changing a Fuse

This appendix shows you how to remove and install fuses for the IP DSLAM.

If you use a fuse other than an included fuse, make sure it matches the fuse specifications in the chapter on product specifications.

Removing a Fuse

Disconnect all power from the IP DSLAM before you begin this procedure.

This process requires partial disassembly of the IP DSLAM. Only a qualified technician should perform this process.

1 Remove the power wires from the IP DSLAM.

2 Remove the IP DSLAM's top cover.

3 See the product specifications for the location of the fuse. A burnt-out fuse is blackened, darkened or cloudy inside its glass casing. A working fuse has a completely clear glass casing.

Use a small flat-head screwdriver to carefully pry out the fuse from the fuse clip.

4 Dispose of the burnt-out fuse properly.

Installing a Fuse

1 Gently press the replacement fuse into the fuse clip until you hear a click.

2 Replace the IP DSLAM's cover.

3 Reconnect the power wires to the unit.

B

Legal Information

Copyright

Disclaimer

ZyXEL does not assume any liability arising out of the application or use of any products, or software described herein. Neither does it convey any license under its patent rights nor the patent rights of others. ZyXEL further reserves the right to make changes in any products described herein without notice. This publication is subject to change without notice.

Trademarks

ZyNOS (ZyXEL Network Operating System) is a registered trademark of ZyXEL Communications, Inc. Other trademarks mentioned in this publication are used for identification purposes only and may be properties of their respective owners.

Certifications

Federal Communications Commission (FCC) Interference Statement

This device complies with Part 15 of FCC rules. Operation is subject to the following two conditions:

- This device may not cause harmful interference.
- This device must accept any interference received, including interference that may cause undesired operations.

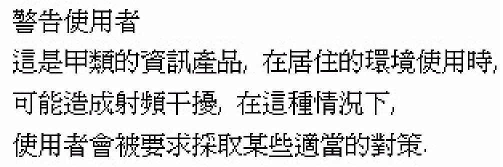
FCC Warning

This device has been tested and found to comply with the limits for a Class A digital switch, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a commercial environment. This device generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instruction manual, may cause harmful interference to radio communications. Operation of this device in a residential area is likely to cause harmful interference in which case the user will be required to correct the interference at his own expense.

CE Mark Warning:

This is a class A product. In a domestic environment this product may cause radio interference in which case the user may be required to take adequate measures.

Taiwanese BSMI (Bureau of Standards, Metrology and Inspection) A Warning:



警告使用者
這是甲類的資訊產品，在居住的環境使用時，
可能造成射頻干擾，在這種情況下，
使用者會被要求採取某些適當的對策．

Notices

Changes or modifications not expressly approved by the party responsible for compliance could void the user's authority to operate the equipment.

This Class A digital apparatus complies with Canadian ICES-003.

Cet appareil numérique de la classe A est conforme à la norme NMB-003 du Canada.

CLASS 1 LASER PRODUCT

APPAREIL A LASER DE CLASS 1

PRODUCT COMPLIES WITH 21 CFR 1040.10 AND 1040.11.

PRODUIT CONFORME SELON 21 CFR 1040.10 ET 1040.11.

Viewing Certifications

1. Go to http://www.zyxel.com.
2. Select your product on the ZyXEL home page to go to that product's page.
3. Select the certification you wish to view from this page.

ZyXEL Limited Warranty

ZyXEL warrants to the original end user (purchaser) that this product is free from any defects in materials or workmanship for a period of up to two years from the date of purchase. During the warranty period, and upon proof of purchase, should the product have indications of failure due to faulty workmanship and/or materials, ZyXEL will, at its discretion, repair or replace the defective products or components without charge for either parts or labor, and to whatever extent it shall deem necessary to restore the product or components to proper operating condition. Any replacement will consist of a new or re-manufactured functionally equivalent product of equal or higher value, and will be solely at the discretion of ZyXEL. This warranty shall not apply if the product has been modified, misused, tampered with, damaged by an act of God, or subjected to abnormal working conditions.

Note

Repair or replacement, as provided under this warranty, is the exclusive remedy of the purchaser. This warranty is in lieu of all other warranties, express or implied, including any implied warranty of merchantability or fitness for a particular use or purpose. ZyXEL shall in no event be held liable for indirect or consequential damages of any kind to the purchaser.

To obtain the services of this warranty, contact your vendor. You may also refer to the warranty policy for the region in which you bought the device at http://www.zyxel.com/web/support_warranty_info.php.

Registration

Register your product online to receive e-mail notices of firmware upgrades and information at www.zyxel.com.

C

Customer Support

In the event of problems that cannot be solved by using this manual, you should contact your vendor. If you cannot contact your vendor, then contact a ZyXEL office for the region in which you bought the device. Regional offices are listed below (see also http://www.zyxel.com/web/contact_us.php). Please have the following information ready when you contact an office.

Required Information

- Product model and serial number.
- Warranty Information.
- Date that you received your device.
- Brief description of the problem and the steps you took to solve it.

"+" is the (prefix) number you dial to make an international telephone call.

Corporate Headquarters (Worldwide)

- Support E-mail: support@zyxel.com.tw
- Sales E-mail: sales@zyxel.com.tw
- Telephone: +886-3-578-3942
- Fax: +886-3-578-2439
- Web: www.zyxel.com
- Regular Mail: ZyXEL Communications Corp., 6 Innovation Road II, Science Park, Hsinchu 300, Taiwan

China - ZyXEL Communications (Beijing) Corp.

- Support E-mail: cso.zycn@zyxel.cn
- Sales E-mail: sales@zyxel.cn
- Telephone: +86-010-82800646
- Fax: +86-010-82800587
- Address: 902, Unit B, Horizon Building, No.6, Zhichun Str, Haidian District, Beijing
- Web: http://www.zyxel.cn

China - ZyXEL Communications (Shanghai) Corp.

- Support E-mail: cso.zycn@zyxel.cn
- Sales E-mail: sales@zyxel.cn
- Telephone: +86-021-61199055
- Fax: +86-021-52069033

- Address: 1005F, ShengGao International Tower, No.137 XianXia Rd., Shanghai
- Web: http://www.zyxel.cn

Costa Rica

- Support E-mail: soporte@zyxel.co.cr
- Sales E-mail: sales@zyxel.co.cr
- Telephone: +506-2017878
- Fax: +506-2015098
- Web: www.zyxel.co.cr
- Regular Mail: ZyXEL Costa Rica, Plaza Roble Escazú, Etapa El Patio, Tercer Piso, San José, Costa Rica

Czech Republic

- E-mail: info@cz.zyxel.com
- Telephone: +420-241-091-350
- Fax: +420-241-091-359
- Web: www.zyxel.cz
- Regular Mail: ZyXEL Communications, Czech s.r.o., Modranská 621, 143 01 Praha 4 - Modrany, Ceská Republika

Denmark

- Support E-mail: support@zyxel.dk
- Sales E-mail: sales@zyxel.dk
- Telephone: +45-39-55-07-00
- Fax: +45-39-55-07-07
- Web: www.zyxel.dk
- Regular Mail: ZyXEL Communications A/S, Columbusvej, 2860 Soeborg, Denmark

Finland

- Support E-mail: support@zyxel.fi
- Sales E-mail: sales@zyxel.fi
- Telephone: +358-9-4780-8411
- Fax: +358-9-4780-8448
- Web: www.zyxel.fi
- Regular Mail: ZyXEL Communications Oy, Malminkaari 10, 00700 Helsinki, Finland

France

- E-mail: info@zyxel.fr
- Telephone: +33-4-72-52-97-97
- Fax: +33-4-72-52-19-20
- Web: www.zyxel.fr
- Regular Mail: ZyXEL France, 1 rue des Vergers, Bat. 1 / C, 69760 Limonest, France

Germany

- Support E-mail: support@zyxel.de
- Sales E-mail: sales@zyxel.de
- Telephone: +49-2405-6909-69
- Fax: +49-2405-6909-99
- Web: www.zyxel.de
- Regular Mail: ZyXEL Deutschland GmbH., Adenauerstr. 20/A2 D-52146, Wuerselen, Germany

Hungary

- Support E-mail: support@zyxel.hu
- Sales E-mail: info@zyxel.hu
- Telephone: +36-1-3361649
- Fax: +36-1-3259100
- Web: www.zyxel.hu
- Regular Mail: ZyXEL Hungary, 48, Zoldlomb Str., H-1025, Budapest, Hungary

India

- Support E-mail: support@zyxel.in
- Sales E-mail: sales@zyxel.in
- Telephone: +91-11-30888144 to +91-11-30888153
- Fax: +91-11-30888149, +91-11-26810715
- Web: http://www.zyxel.in
- Regular Mail: India - ZyXEL Technology India Pvt Ltd., II-Floor, F2/9 Okhla Phase -1, New Delhi 110020, India

Japan

- Support E-mail: support@zyxel.co.jp
- Sales E-mail: zyp@zyxel.co.jp
- Telephone: +81-3-6847-3700
- Fax: +81-3-6847-3705
- Web: www.zyxel.co.jp
- Regular Mail: ZyXEL Japan, 3F, Office T&U, 1-10-10 Higashi-Gotanda, Shinagawa-ku, Tokyo 141-0022, Japan

Kazakhstan

- Support: http://zyxel.kz/support
- Sales E-mail: sales@zyxel.kz
- Telephone: +7-3272-590-698
- Fax: +7-3272-590-689
- Web: www.zyxel.kz
- Regular Mail: ZyXEL Kazakhstan, 43 Dostyk Ave., Office 414, Dostyk Business Centre, 050010 Almaty, Republic of Kazakhstan

Malaysia

- Support E-mail: support@zyxel.com.my
- Sales E-mail: sales@zyxel.com.my
- Telephone: +603-8076-9933
- Fax: +603-8076-9833
- Web: http://www.zyxel.com.my
- Regular Mail: ZyXEL Malaysia Sdn Bhd., 1-02 & 1-03, Jalan Kenari 17F, Bandar Puchong Jaya, 47100 Puchong, Selangor Darul Ehsan, Malaysia

North America

- Support E-mail: support@zyxel.com
- Support Telephone: +1-800-978-7222
- Sales E-mail: sales@zyxel.com
- Sales Telephone: +1-714-632-0882
- Fax: +1-714-632-0858
- Web: www.zyxel.com
- Regular Mail: ZyXEL Communications Inc., 1130 N. Miller St., Anaheim, CA 92806-2001, U.S.A.

Norway

- Support E-mail: support@zyxel.no
- Sales E-mail: sales@zyxel.no
- Telephone: +47-22-80-61-80
- Fax: +47-22-80-61-81
- Web: www.zyxel.no
- Regular Mail: ZyXEL Communications A/S, Nils Hansens vei 13, 0667 Oslo, Norway

Poland

- E-mail: info@pl.zyxel.com
- Telephone: +48-22-333 8250
- Fax: +48-22-333 8251
- Web: www.pl.zyxel.com
- Regular Mail: ZyXEL Communications, ul. Okrzei 1A, 03-715 Warszawa, Poland

Russia

- Support: http://zyxel.ru/support
- Sales E-mail: sales@zyxel.ru
- Telephone: +7-095-542-89-29
- Fax: +7-095-542-89-25
- Web: www.zyxel.ru
- Regular Mail: ZyXEL Russia, Ostrovityanova 37a Str., Moscow 117279, Russia

Singapore

- Support E-mail: support@zyxel.com.sg
- Sales E-mail: sales@zyxel.com.sg
- Telephone: +65-6899-6678
- Fax: +65-6899-8887
- Web: http://www.zyxel.com.sg
- Regular Mail: ZyXEL Singapore Pte Ltd., No. 2 International Business Park, The Strategy #03-28, Singapore 609930

Spain

- Support E-mail: support@zyxel.es
- Sales E-mail: sales@zyxel.es
- Telephone: +34-902-195-420
- Fax: +34-913-005-345
- Web: www.zyxel.es
- Regular Mail: ZyXEL Communications, Arte, 21 5ª planta, 28033 Madrid, Spain

Sweden

- Support E-mail: support@zyxel.se
- Sales E-mail: sales@zyxel.se
- Telephone: +46-31-744-7700
- Fax: +46-31-744-7701
- Web: www.zyxel.se
- Regular Mail: ZyXEL Communications A/S, Sjöporten 4, 41764 Göteborg, Sweden

Taiwan

- Support E-mail: support@zyxel.com.tw
- Sales E-mail: sales@zyxel.com.tw
- Telephone: +886-2-27399889
- Fax: +886-2-27353220
- Web: http://www.zyxel.com.tw
- Address: Room B, 21F., No.333, Sec. 2, Dunhua S. Rd., Da-an District, Taipei

Thailand

- Support E-mail: support@zyxel.co.th
- Sales E-mail: sales@zyxel.co.th
- Telephone: +662-831-5315
- Fax: +662-831-5395
- Web: http://www.zyxel.co.th
- Regular Mail: ZyXEL Thailand Co., Ltd., 1/1 Moo 2, Ratchaphruk Road, Bangrak-Noi, Muang, Nonthaburi 11000, Thailand.

Turkey

- Support E-mail: cso@zyxel.com.tr
- Telephone: +90 212 222 55 22
- Fax: +90-212-220-2526
- Web: http:www.zyxel.com.tr
- Address: Kaptanpasa Mahallesi Piyalepasa Bulvari Ortadogu Plaza N:14/13 K:6 Okmeydani/Sisli Istanbul/Turkey

Ukraine

- Support E-mail: support@ua.zyxel.com
- Sales E-mail: sales@ua.zyxel.com
- Telephone: +380-44-247-69-78
- Fax: +380-44-494-49-32
- Web: www.ua.zyxel.com
- Regular Mail: ZyXEL Ukraine, 13, Pimonenko Str., Kiev 04050, Ukraine

United Kingdom

- Support E-mail: support@zyxel.co.uk
- Sales E-mail: sales@zyxel.co.uk
- Telephone: +44-1344-303044, 0845 122 0301 (UK only)
- Fax: +44-1344-303034
- Web: www.zyxel.co.uk
- Regular Mail: ZyXEL Communications UK Ltd., 11 The Courtyard, Eastern Road, Bracknell, Berkshire RG12 2XB, United Kingdom (UK)

Index